GSDC
Global Skill Development Council

Globally Recognised Certification Body
190+ countries · 2,50,000+ Certified Professionals

IAF MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT

IAS ACCREDITED Personnel Certification Body

AI Governance Framework Guide

www.gsdcouncil.org

1. The Rise of AI Governance

1.1 Background

Artificial intelligence now sits at the centre of critical business decisions — from credit scoring and medical diagnostics to supply chain optimisation and hiring. As AI systems grow in capability and reach, the stakes of deploying them irresponsibly escalate in equal measure. **Governance** has emerged as the essential discipline that bridges the gap between rapid technological innovation and the demand for accountability.

1.2 The Role of Frameworks

Frameworks provide organisations with a structured baseline for responsible AI deployment. Rather than leaving ethical and operational questions to chance, they offer repeatable processes, clear roles, and measurable standards — enabling organisations to move forward with confidence.

1.3 Core Governance Imperatives

1. **Innovation.** Frameworks enable bold AI adoption without sacrificing oversight.
2. **Risk.** Structured governance identifies and mitigates AI-specific harms.
3. **Trust.** Transparent practices build durable stakeholder confidence.

2. ISO/IEC 42001: The AIMS Standard

2.1 Overview

ISO/IEC 42001 represents a landmark moment in the history of AI regulation. Published in December 2023 by the **International Organisation for Standardisation (ISO)** and the **International Electrotechnical Commission (IEC)**, it is the world's first certifiable **Artificial Intelligence Management System (AIMS)** standard. It provides organisations with a structured framework to develop, implement, maintain, and continually improve their approach to responsible AI development and use.

2.2 Design for Integration

A key strength of ISO/IEC 42001 is its design for integration. It follows the same high-level structure (**Annex SL**) as other popular ISO management systems, making it straightforward to incorporate alongside existing governance structures without duplication. Compatible standards include:

1. ISO 9001 — Quality Management
2. ISO 27001 — Information Security Management
3. ISO 14001 — Environmental Management

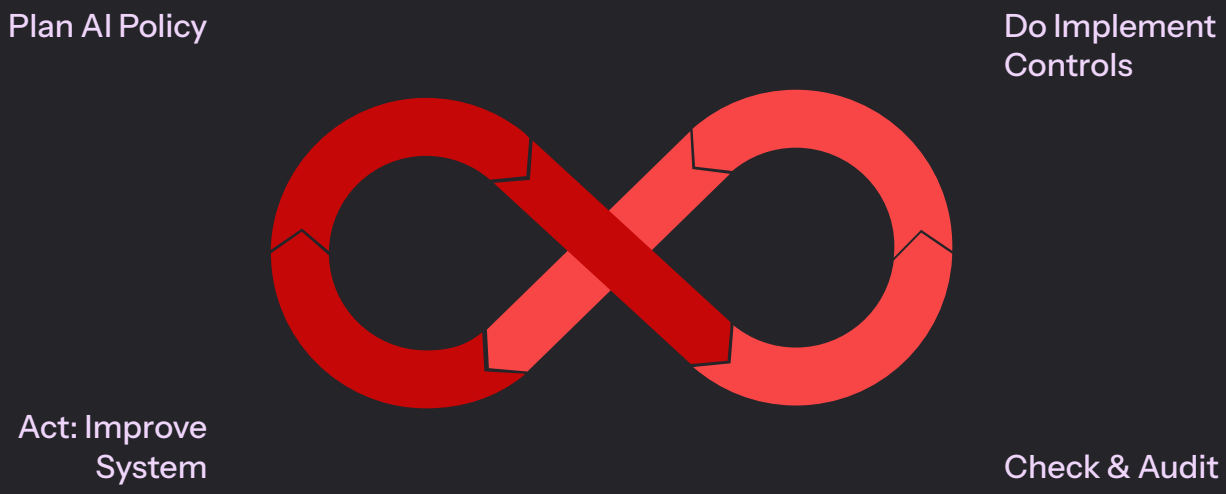
2.3 Key Facts

1. **Publication date:** December 2023
2. **Publishers:** ISO and IEC (jointly)
3. **Scope:** First certifiable AI management standard
4. **Harmonisation:** Aligned with ISO 9001 and ISO 27001
5. **Applicability:** All organisation sizes

2.1 ISO/IEC 42001 Structure

2.1.1 The Plan-Do-Check-Act Cycle

The standard is built upon the universally recognised **Plan-Do-Check-Act (PDCA)** cycle, ensuring that AI governance is treated as a dynamic, continuously improving discipline rather than a one-time compliance exercise.



2.1.2 Structural Components

2.1.2.1 Ten Clauses. The standard is structured across ten clauses — from context of the organisation through to improvement — each defining clear requirements for AI governance at every level.

2.1.2.2 Certification Readiness. Mandatory controls and documented evidence requirements are designed specifically to support third-party certification audits, giving organisations a credible, demonstrable badge of conformity.

2.2 Key Requirements of ISO/IEC 42001

ISO/IEC 42001 places significant emphasis on embedding AI governance into the culture and operational fabric of the organisation, not merely its documentation. Three pillars underpin certification readiness.

2.2.1 Leadership Commitment

Top management must visibly champion the **AI Management System** by defining an AI policy, assigning accountability, and allocating adequate resources. Governance without executive sponsorship is governance in name only.

2.2.2 Systematic Risk Assessment

Organisations must conduct structured AI risk assessments covering the following dimensions:
i. Data quality
ii. Model reliability
iii. Ethical implications
iv. Downstream impacts

Appropriate risk treatment controls are then selected and applied from **Annex A**.

2.2.3 Continual Improvement

The management system must evolve through the following mechanisms:
i. Regular internal audits
ii. Management reviews
iii. Corrective action processes

This ensures the organisation keeps pace with AI developments and emerging regulatory expectations.

3. NIST AI Risk Management Framework

3.1 Key Characteristics

1. Voluntary, non-prescriptive guidance
2. Released by NIST, January 2023
3. Sector and size agnostic
4. Focused on AI-specific risk dimensions
5. Freely available and openly maintained

The **National Institute of Standards and Technology (NIST) AI Risk Management Framework** offers a flexible, voluntary approach to identifying, measuring, and managing the risks associated with AI systems. Released in January 2023, it was developed through extensive public consultation and reflects a broad cross-sector consensus on what trustworthy AI looks like in practice.

Unlike **ISO 42001**, the **NIST AI RMF** is descriptive rather than prescriptive — it does not mandate specific controls but instead provides a common language and structured approach that any organisation, regardless of sector or scale, can adapt to its own context.

3.2 The Four Core Functions of the NIST AI RMF

At the heart of the **NIST AI Risk Management Framework** are four core functions — **Govern**, **Map**, **Measure**, and **Manage** — which together form a comprehensive risk lifecycle covering strategy, context, evaluation, and action.

1. **Govern** — Establish culture, accountability, and strategic policies for AI risk management.
2. **Map** — Understand the system context, stakeholders, and potential risk landscape.
3. **Measure** — Quantify trustworthiness, evaluate bias, and track performance metrics.
4. **Manage** — Allocate resources, deploy controls, and respond to incidents effectively.

3.2 The Four Functions of NIST AI RMF

The **NIST AI Risk Management Framework** is structured around four core functions — **Govern**, **Map**, **Measure**, and **Manage** — each addressing a distinct phase of the AI risk lifecycle, from strategic oversight and context-setting through to evaluation and active risk response.

1. Govern

Establish the culture, accountability structures, and strategic policies that underpin responsible AI risk management across the organisation.

2. Map

Understand the AI system's context, identify relevant stakeholders, and characterise the potential risk landscape before deployment.

3. Measure

Quantify trustworthiness, evaluate bias and fairness, and track key performance and safety metrics throughout the system lifecycle.

4. Manage

Allocate resources, implement controls, and respond effectively to AI-related incidents and emerging risks as they arise.

3.2.1 Govern: The Foundation of Oversight

The **Govern** function establishes the organisational conditions necessary for effective AI risk management. It is not merely a policy exercise — it demands that leadership actively shape the values, structures, and accountabilities that govern how AI is used across the enterprise.

The Govern function encompasses three primary imperatives:

1. **3.2.1.1 Define Roles and Responsibilities.** Clear accountability structures ensure that no aspect of AI risk falls through the cracks between teams or departments.
2. **3.2.1.2 Align AI with Organisational Values.** AI use cases must be evaluated against legal obligations, ethical principles, and stated organisational commitments.
3. **3.2.1.3 Foster Responsible Innovation Culture.** Governance mechanisms should empower teams to raise concerns and flag emerging risks without fear of reprisal.

3.2.2 Map: Understanding the Ecosystem

Before risks can be assessed, they must be understood in full context. The **Map** function directs organisations to systematically characterise their AI systems, the environments in which they operate, and the full range of stakeholders who may be affected by their outputs.

The Map function encompasses three principal areas of inquiry:

1. **3.2.2.1 Stakeholder Identification.** Mapping who is affected by an AI system — including end-users, impacted communities, and regulators — is essential to understanding the full risk surface.
2. **3.2.2.2 Technical Capabilities and Limits.** Understanding where a model performs reliably and where it is prone to failure is fundamental to responsible deployment decisions.
3. **3.2.2.3 Anticipating Misuse.** Organisations must consider how their AI systems might be used beyond their intended purpose, including adversarial and accidental misuse scenarios.

3.2.3 Measure: Quantifying Trustworthiness

The **Measure** function transforms abstract commitments to trustworthy AI into concrete, evidence-based evaluations. It requires organisations to apply rigorous testing and monitoring methodologies that cover the full spectrum of AI trustworthiness characteristics.

Testing for bias and fairness, evaluating accuracy across demographic subgroups, and assessing robustness against adversarial inputs are all central activities. Equally important is establishing ongoing monitoring to detect **performance drift** — the gradual degradation of model quality as real-world data distributions shift over time.

3.2.3.1 Core Measurement Areas

1. **Accuracy and Bias:** Systematic evaluation across demographic subgroups to ensure equitable model performance.
2. **Performance Drift:** Ongoing monitoring as real-world conditions evolve and data distributions shift over time.
3. **Explainability:** Ensuring model outputs can be interpreted and justified by relevant stakeholders.

3.2.4 Manage: Implementing Controls

3.2.4.1 Overview

The **Manage** function translates risk analysis into decisive action. Having mapped and measured risks, organisations must now deploy the technical safeguards, operational procedures, and contingency plans needed to keep AI systems operating within acceptable risk tolerances.

3.2.4.2 Core Management Activities

1. **Deploy Safeguards.** Technical controls, input validation, and output monitoring mechanisms limit the impact of model failures.
2. **Incident Response.** Documented procedures for detecting, escalating, and correcting AI errors ensure rapid, coordinated action when things go wrong.
3. **Change Management.** Version control, re-validation requirements, and change logs maintain audit trails through the full model lifecycle.

4. ISO/IEC 23894: AI Risk Management

4.1 Overview

ISO/IEC 23894 extends the well-established principles of **ISO 31000** — the international standard for risk management — into the specific domain of artificial intelligence. It recognises that AI systems present risk characteristics that generic risk frameworks were not designed to address: opacity in decision-making, deep dependence on training data quality, and the dynamic behaviour of systems that learn and adapt over time.

The standard provides operational guidance for identifying, analysing, evaluating, and treating AI-specific risks throughout the system lifecycle. It is particularly valuable for organisations implementing **ISO/IEC 42001** who need detailed risk management methodology to meet their AIMS obligations.

4.2 AI-Specific Risk Characteristics

1. **Opacity:** Black-box model behaviour
2. **Data dependency:** Bias from training data
3. **Learning dynamics:** Behaviour shift post-deployment
4. **Emergent properties:** Unpredicted capabilities

5. ISO/IEC 38507: Governance of IT for AI

5.1 Overview

While **ISO/IEC 42001** addresses AI management at the operational and organisational level, **ISO/IEC 38507** occupies a distinct strategic position — it is written for governing bodies and boards, equipping them with the tools needed to understand and discharge their responsibilities regarding AI use within their organisations.

5.2 Key Functions

1. Board-Level Decision Making

The standard provides governing bodies with a structured approach to evaluating, directing, and monitoring the organisation's use of AI — without requiring deep technical expertise.

2. Strategic AI Interpretation

It equips boards with tools to interpret the governance implications of AI — from liability and reputation to ethics and regulatory exposure.

3. Complementarity with ISO 42001

Where ISO 42001 addresses operational management, ISO 38507 ensures that top-level strategy and board oversight keep pace, creating a coherent governance architecture from board to practitioner.

6. OECD AI Principles

6.1 Overview

The **OECD AI Principles** represent one of the most broadly adopted intergovernmental statements on responsible AI. They have been integrated into national AI strategies across more than 40 countries and provide the conceptual foundation for a wave of subsequent legislation and regulation — including the EU AI Act.

6.2 Core Principles

1. **Inclusive Growth** — AI should benefit all people and promote sustainable development.
2. **Human Rights** — AI must respect the rule of law, democracy, and human dignity.
3. **Transparency** — AI actors must ensure traceability and intelligibility of systems.
4. **Safety & Security** — AI systems must be robust and safe throughout their lifecycle.
5. **Accountability** — AI actors must be held responsible for the proper functioning of AI.

7. UNESCO Recommendation on the Ethics of Artificial Intelligence

7.1 Scope and Reach

1. Adopted unanimously in November 2021
2. 194 UNESCO member states committed
3. First global normative instrument on AI ethics
4. Mandatory AI ethics impact assessments called for
5. Explicit protection of vulnerable groups

7.2 Overview

The **UNESCO Recommendation on the Ethics of AI** is the most geographically comprehensive normative framework in the AI governance landscape. Adopted unanimously by 194 member states, it centres on the protection and promotion of human rights and human dignity as non-negotiable conditions for AI development.

7.3 Key Mechanisms and Provisions

Critically, UNESCO calls for all member states to conduct comprehensive **AI ethics impact assessments** before deploying AI in sensitive contexts — a mechanism designed to surface potential harms to individuals and communities before they materialise at scale. The framework also explicitly addresses the following domains:

1. Data governance and stewardship
2. Environmental sustainability of AI systems
3. Protection of children and marginalised groups

8. Comparative Analysis of AI Governance Frameworks

8.1 Scope and Focus

Each major AI governance framework occupies a distinct position in the landscape. Understanding their scope, purpose, and approach enables organisations to make informed decisions about which to adopt — and how to combine them effectively.

Dimension	NIST AI RMF	ISO/IEC 42001	OECD / UNESCO
Nature	Voluntary & descriptive	Prescriptive & certifiable	Principled & normative
Audience	All US & global organisations	All organisations seeking cert.	Governments & policy makers
Primary Focus	Risk identification & management	Management system maturity	Ethics & human rights
Certification	No	Yes	No
Best Used For	Risk assessment & benchmarking	Formal compliance & audit	Policy & values alignment

9. Harmonising Governance Efforts

Far from being competing alternatives, the major AI governance frameworks are designed to be complementary. Smart organisations build unified governance strategies that draw on the strengths of each, using established crosswalks and mapping tools to prevent duplication and maximise coverage.

9.1 Integration Methodology

1. **Map Conceptual Overlaps.** Identify where NIST AI RMF functions align with ISO 42001 clauses and OECD principles to avoid redundant documentation and controls.
2. **Leverage Official Crosswalks.** NIST and ISO have published mapping documents that trace equivalencies between their respective frameworks, enabling efficient dual compliance.
3. **Build a Unified Strategy.** Consolidate policies, controls, and evidence repositories into a single, defensible governance programme that satisfies multiple frameworks simultaneously.

10. Selecting the Right Framework

Choosing an AI governance framework is not a one-size-fits-all decision. The right starting point depends on organisational maturity, regulatory environment, commercial requirements, and strategic ambitions. The following criteria provide a structured approach to framework selection.

10.1 Framework Selection Criteria

1. **Assess Organisational Maturity**
    a. Evaluate existing organisational capability and readiness
    b. Review alignment with current management systems
    c. Appraise the prevailing risk culture and governance structures
2. **Determine Regulatory and Commercial Need**
    a. Identify applicable sector-specific regulatory requirements
    b. Assess exposure to and obligations under the **EU AI Act**
    c. Review client contractual and due diligence requirements
3. **Layer Governance Approaches Strategically**
    a. Deploy the **NIST AI RMF** for internal assessment and benchmarking purposes
    b. Pursue **ISO 42001** certification where formal third-party assurance is required
    c. Apply **OECD** and **UNESCO** principles to reinforce ethical alignment and values-based governance

Organisations operating in the EU should also assess alignment with the **EU AI Act**, which references ISO standards as a path to demonstrating conformity.

11. The Future of AI Compliance

11.1 From Voluntary to Mandatory

The era of purely voluntary AI governance is drawing to a close. The **EU AI Act** — the world's first comprehensive binding AI regulation — creates legal obligations for high-risk AI systems and explicitly references harmonised standards, including **ISO/IEC 42001**, as pathways to demonstrating conformity. Other jurisdictions are moving in the same direction.

11.2 Standards as Compliance Currency

ISO and **NIST** standards are rapidly becoming the de facto currency of AI compliance. Certification to ISO/IEC 42001, in particular, is expected to function as evidence of conformity with regulatory requirements across multiple jurisdictions — reducing the burden of demonstrating compliance to individual regulators.

11.3 Implications for Governance Strategy

As AI capabilities continue to advance — with generative models, autonomous agents, and foundation models introducing genuinely novel risk profiles — governance frameworks will need to evolve with equal agility. Organisations that build adaptive, standards-aligned governance systems today will be best positioned to meet tomorrow's mandatory expectations.

Conclusion: Building Trust Through Governance

> Governance is not a constraint on innovation — it is the foundation upon which sustainable, trustworthy AI is built.

The frameworks explored in this document — **ISO/IEC 42001**, the **NIST AI RMF**, **ISO/IEC 23894**, **ISO/IEC 38507**, the **OECD AI Principles**, and the **UNESCO AI Ethics Recommendation** — collectively represent the global consensus on what responsible AI looks like in practice. No single framework provides all the answers, but together they chart a clear path.

1	2	3
Continuous Improvement Governance is a living discipline. Commit to regular review, audit, and adaptation as AI and regulation evolve.	**Structured Pathways** International standards provide proven, auditable pathways to responsible innovation — use them as your foundation.	**Transparency First** Demonstrable transparency in AI decision-making is the single most powerful tool for securing long-term stakeholder trust.

GSDC Global Skill Development Council

Globally Recognised Certification Body
190+ countries · 2,50,000+ Certified Professionals

IAF MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT

IAS ACCREDITED Personnel Certification Body

CERTIFIED AI GOVERNANCE PROFESSIONAL

ABOUT GSDC CERTIFICATION

EBOOK

Extensive and exclusive Ebook created by world's experts to help you with understanding core concepts.

LEARNING MATERIALS

Get access to learning materials such as videos, ebooks, templates, and practice exams, which will help you clear the certification exam.

CREATED BY EXPERTS

GSDC certifications are created and authored by world's leading experts in the field.

LEARNING OBJECTIVE

- Gain a strong understanding of AI governance principles and practices
- Apply AI governance concepts to real-world organizational needs
- Develop skills to identify and manage AI-related risks
- Build effective AI governance practices for responsible AI adoption

Enroll now with the code **LEARN20** To avail **20%** discount

Enroll Now

www.gsdcouncil.org