



Ministry of Communications
and Information Technology



Egyptian Center for Responsible AI

Global AI Governance Frameworks

A Comparative Study



Table of Contents

1 Executive Summary	3
1.1 Key Findings	3
1.2 Strategic Conclusion	5
2 Introduction	6
2.1 Background and Rationale	6
2.2 Objectives of the Study	7
2.3 Methodology and Analytical Framework	7
2.4 Data Sources	8
2.5 Scope and Limitations	8
3 International and Regional Governance Landscapes	9
3.1 Landscape Mapping - The Three Tiers of Influence	9
3.2 Regional and International Lever - Comparative Analysis Matrix	11
3.3 The «Global South» Perspective	12
3.4 Strategic Implications for the Egyptian Framework	13
3.5 Conclusion	13
4 National AI Governance Landscapes	14
4.1 Landscape Mapping - The Four Classification Models	14
4.2 National Level - Consolidated Comparative Matrix	16
4.3 Key Areas of Global Convergence and Divergence	18
4.4 Critical Comparative Insights	20
4.5 Inherent Structural Challenges	21
4.6 Conclusion	22
5 Sectoral AI Governance Landscapes	24
5.1 Landscape Mapping- Three Classification Models	24
5.2 Sectoral Level - Consolidated Comparative Matrix	26
5.3 Key Areas of Global Convergence and Divergence	26
5.4 Critical Comparative Insights	27
5.5 Inherent Structural Challenges	28
5.6 Conclusion	28
6 References and Appendices	29
6.1 References	29
6.2 Appendices	56
Appendix A: Glossary of Key Terms	56
Appendix B: Glossary of Consolidated Comparative Matrix – National Level	57
Appendix C: Glossary of Consolidated Comparative Matrix – Sectoral Level	59
Appendix D: Abbreviations and Acronyms	61
Appendix E: Key data points for the National AI governance framework	64
Appendix F: Key data points for Regional and International AI Governance Entities	73
Appendix G: Detailed Profiles of Sectoral Regulations	113
Appendix H: Detailed Profiles of Sectoral Regulations	128

1 Executive Summary

The global landscape of Artificial Intelligence (AI) governance has fundamentally shifted: the era of abstract “principles” is ending, and the era of “implementation” has begun. As nations and industries race to harness the economic potential of AI, the regulatory environment is no longer defined by a simple binary choice between innovation and regulation.

To map this transition, this study presents a comparative analysis of global AI governance, examining 35 frameworks across the **Regional and International, National, and Sectoral** levels. The analysis reveals that the global landscape has matured beyond the binary choice between “innovation” and “regulation,” evolving instead into a complex **“Three-Tiered Reality,”** “and that successful governance now requires navigating a complex, multi-layered ecosystem where legal mandates, geopolitical alliances, and sectoral risk profiles intersect.

1.1 Key Findings

A. The Global “Compliance Divide.”

The analysis of 14 international and regional organizations reveals a sharp divide between the Global North and the Global South. While the EU and OECD focus on “Market Safety” and “Trade Interoperability”, the African Union and BRICS prioritize “Digital Sovereignty” and “Infrastructure Independence”.

Strategic Insight: Emerging economies must pursue a “Multi-Tiered Alignment” strategy—adopting developed countries’ trade standards (OECD) for export viability, while leveraging Global South alliances (BRICS/AU/LAS ...) to build sovereign infrastructure.

B. The Rise of “Hybrid” National Models

The analysis of 14 countries demonstrates that high-growth emerging economies (e.g., India, Saudi Arabia, UAE) are rejecting the binary choice between “Pro-Innovation” and “Statutory” regimes.

Strategic Insight: These nations are actively engineering “Hybrid/Strategic” models. They utilize “soft law” and sandboxes to foster private innovation while enforcing strict “hard law” on government data and national security, effectively balancing growth with control.

The Hybrid Model Architecture: A Structural Diagram



C. Operational Convergence via Standards

There is a common agreement on technical standards. Frameworks like ISO/IEC 42001 and the NIST AI Risk Management Framework are emerging as the universal “common language,” allowing nations to ensure interoperability regardless of their domestic legal structures. National standardization bodies of might strive at different levels to ensure a degree interoperability, while influencing the standards developed internationally.

Strategic Insight: Policymakers should decouple “technical compliance” from “political regulation.” Adopting international standards (ISO/NIST/ITU/IEE and others) creates an immediate “Trade Lane” for local AI exports, effectively bypassing the need for complex international treaties to ensure market access.

D. Governance as a National Strategy Tool

Successful frameworks are not “copy-paste” solutions; they are engineered to solve specific national challenges.

- Brazil utilizes governance to address social inequality.
- China structures its framework around state security and information control.
- Saudi Arabia & UAE treat AI governance as a pillar of economic diversification (e.g., Vision 2030).

Strategic Insight: Governance must be reverse-engineered from national KPIs. If the priority is attracting Foreign Direct Investment (FDI), the framework should prioritize “Soft Law” flexibility; if the priority is national security, it must prioritize “Statutory” control. One size does not fit all.

E. Certification as a “Global Trade Passport.”

For industrial sectors, international AI certification is now the de facto law of the market. Achieving ISO 42001 (Management) and ISO 27001 (Security) certification is essential for integration into global supply chains.

Strategic Insight: For export-oriented industries (like Manufacturing and Energy), meeting government regulations is secondary to meeting supply chain requirements. Certification acts as a “Trade Passport” that supersedes domestic laws, granting access to global buyers who demand rigorous third-party verification.

F. The “Three-Tiered” Sectoral Reality

The analysis of 7 critical sectors confirms that governance is not uniform; they are categorized by risk levels. Industries are organized into three compliance tiers:

- High-Stakes (e.g., Health, Fintech): Governed by binding, mandatory statutes.
- Industrial (e.g., Energy, Manufacturing): Governed by international standards (ISO/IEC 42001).
- Emerging (e.g., Education, Agriculture): Governed by strategic soft law to encourage adoption.

Strategic Insight: National frameworks must be **modular**, allowing strict enforcement for high-stakes domains while opting for a “sandbox” environment for emerging sectors to avoid stifling innovation.

G. The “Horizontal” Shift: Function Over Label

Modern regulations like the **EU AI Act** are “horizontal”—they regulate the function of the AI, not the sector label.

Strategic Insight: Leaders must assess compliance based on AI function, not business sector. If a farm uses AI to hire staff, it triggers the same high-risk laws as a tech giant. Ignoring this distinction leaves the organization vulnerable to severe regulatory penalties.

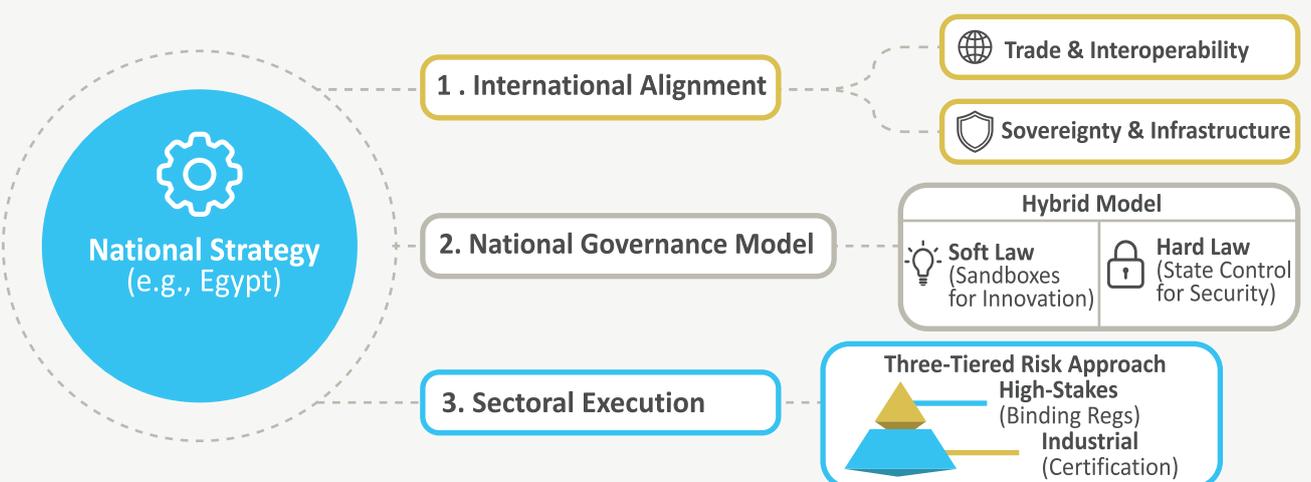
1.2 Strategic Conclusion

The comparative evidence confirms that the “Best Practice” for an emerging ecosystem is not to copy a single foreign model, but to engineer a Strategic Hybrid.

- **Nationally**, this requires balancing “Soft Law” flexibility for innovation with “Hard Law” mandates for state sovereignty.
- **Internationally**, it requires a “Multi-Tiered Alignment”—adopting developed countries’ recommendations/ standards for trade interoperability while leveraging Global South alliances for infrastructure independence.
- **Sectorally**, it requires recognizing that compliance is no longer one-size-fits-all but varies directly with risk.

Ultimately, successful governance depends on integrating these layers to ensure safety without stifling the development of a sovereign AI ecosystem.

Integrated National Strategy Blueprint: A Cohesive Plan for Emerging Economies



2 Introduction

2.1 Background and Rationale

Artificial intelligence is among the most transformative technologies of the 21st century, with the potential to reshape economies, societies, and governance systems worldwide. As AI systems become more powerful and pervasive—from large language models and generative AI to autonomous vehicles and medical diagnostics—they offer immense opportunities for economic growth, scientific discovery, and social progress. However, they also pose significant risks, including algorithmic bias, privacy violations, job displacement, threats to public safety, and challenges to fundamental rights and democratic values.

In response to these opportunities and risks, governments, international organizations, industry bodies, and civil society groups worldwide are developing an increasingly complex web of governance frameworks. These frameworks range from high-level ethical principles and voluntary guidelines to comprehensive, legally binding regulations. They operate at multiple levels—national, regional, international, and sectoral—and reflect diverse legal traditions, political systems, economic priorities, and social values.

The rapid proliferation of these frameworks has created a fragmented and often confusing landscape. Policymakers struggle to understand how different approaches compare and which models are most effective for their specific contexts. Industry leaders face the challenge of navigating a patchwork of overlapping and sometimes contradictory requirements. Researchers and civil society organizations aim to identify best practices and advocate for governance approaches that genuinely safeguard public interests.

The Evolution of AI Governance: From Principles to Implementation



Figure 3: Evolution of AI Governance

This study presents these challenges by providing a comprehensive, multi-layered comparative analysis of the global AI governance landscape. It examines frameworks at the national, regional, international, and sectoral levels, identifying key models, trends, and dynamics. By integrating these different perspectives into a single analysis, the report provides a comprehensive understanding of how the world governs AI and offers strategic insights for all stakeholders seeking to navigate this complex terrain.

2.2 Objectives of the Study

This study has four primary objectives:

- **Mapping the Governance Landscape:** The report analyzes 35 frameworks across three domains—National (14), Regional/International (14), and Sectoral (7) — and classifies them into regulatory archetypes.
- **Distilling Strategic Models:** It identifies how nations create “Strategic Hybrids” by balancing “soft law” flexibility for innovation with “hard” mandates for sovereignty.
- **Analyzing Convergence and Divergence:** The report distinguishes between areas of political divergence and operational convergence, identifying universal standards.
- **Evaluating Trade-offs and Risks:** It critically assesses the “Structural Defects” within each model, such as the “Bureaucracy Trap,” offering decision-makers insight into potential pitfalls when applying these models in emerging ecosystems.

2.3 Methodology and Analytical Framework

This study employs a structured Regulatory Analysis methodology. Rather than viewing governance initiatives in isolation, the study applies a consistent “Taxonomy of Regulation” to classify frameworks into distinct models.

The analysis is conducted across three levels—Regional & International (14 organizations), National (14 countries), and Sectoral (7 industries)—examining each against a standardized matrix of seven key governance dimensions:

- **Regulatory Archetype (The Model):** Classifying the framework into a specific governance family (e.g., “Pro-Innovation,” “Statutory/Risk-Based,” or “Hybrid/Strategic”) based on its philosophical approach to state control.
- **Legal Nature & Status:** Determining the binding force of the framework, distinguishing between mandatory statutes (“Hard Law”), voluntary guidance (“Soft Law”), and hybrid approaches.
- **Domain & Scope:** Analyzing the precise applicability of the rules—whether they apply strictly to the public sector, the private sector, or specific high-stakes functions.
- **Regulatory Approach:** Identifying the state’s mechanism for management, such as “Agile/Sandboxing,” “Pre-Market Approval,” or “Sector-Led” oversight.
- **Risk Management Methodology:** Evaluating how risk is calculated—distinguishing between rigid “Risk-Tiered” lists (e.g., EU model) and continuous “Process-Based” lifecycles (e.g., NIST/ISO model).
- **Enforcement & Compliance:** Mapping the tools used to enforce the rules, ranging from central authority audits and fines to third-party certifications and reputational pressure.
- **Structural Defect Analysis (The “Trap”):** A critical risk assessment that identifies the inherent trade-offs and “hidden defects” within each model (e.g., the “Bureaucracy Trap” vs. the “Regulatory Vacuum”).

2.4 Data Sources

The analysis draws on primary source documents, including official legislative texts (Acts/Bills), national strategies, international standards (ISO/IEC), and technical policy frameworks.

2.5 Scope and Limitations

Scope

This study provides a comparative analysis of 35 distinct governance frameworks organized across three levels:

1. International & Regional Level: 14 frameworks analyzed by their functional influence on global policy.

These entities are the UN, the OECD, UNESCO, ITU, G7, G20, GPAI, the Council of Europe, the European Union (EU AI Act), the African Union (AU), the League of Arab States (AICTO), BRICS, ASEAN, the Organization of Islamic Cooperation (OIC), and Latin America & the Caribbean (LAC).

2. National Level: 14 representative countries selected to illustrate distinct regulatory regions (Latin America, North America, Europe, the Asia-Pacific, Africa, and the Arab Region).

Countries: Brazil, Canada, China, Finland (EU Representative), India, Japan, Kenya, Saudi Arabia, Singapore, South Africa, South Korea, United Arab Emirates, United Kingdom, United States.

3. Sectoral Level: 7 business sectors selected to represent varying degrees of risk and governance maturity.

Sectors: Healthcare, Education, Agriculture, Energy, Fintech, Transportation, Manufacturing.

Limitations

While this study offers a robust mapping of the global landscape, it is subject to the following structural limitations:

First, the AI governance landscape is rapidly evolving, with new frameworks emerging and existing ones being updated regularly. This analysis reflects the state of the field as of November 2025.

Second, the selection of countries and frameworks, while comprehensive, is not exhaustive. Many countries and regions are developing AI governance approaches that are not covered in detail here.

Third, the analysis focuses primarily on formal governance frameworks and may not fully capture informal norms, industry self-regulation, or civil society initiatives.

3 International and Regional Governance Landscapes

This section analyzes 14 major international and regional organizations, categorized not by geography but by their **functional influence** on global policy. The research highlights a fundamental shift from abstract ethical principles to geopolitical implementation, revealing a distinct **“Compliance Divide”**.

While **Global Norm-Setters** (like the OECD and ITU) and the **Regulatory Anchor** (EU AI Act) establish the baselines for trade interoperability and safety, **Regional Alliances** (such as the AU and BRICS) provide the counter-narrative of “Digital Sovereignty”. This chapter maps these frameworks to identify the critical structural gaps—specifically in infrastructure and data representation—that emerging economies must navigate. The analysis suggests a **“Multi-Tiered Alignment”** strategy, leveraging developed countries’ standards for trade while utilizing Global South frameworks to build sovereign capacity.

3.1 Landscape Mapping - The Three Tiers of Influence

To assist in navigating these frameworks, we have categorized organizations not by geography but by their possible **functional influence** on the AI Egyptian policy.



Figure 4: Three tiers of Regional & International Influence on Egyptian Policy

Tier 1: The Global Norm-Setters (Soft Law & Trade)

These organizations set the “**baseline**” for international trade and cooperation.

- **OECD:** The primary standard for economic interoperability. Its principles are the foundation for the G20 and G7 processes. Adherence here is voluntary but essential for integration into global digital economies. 

- **UNESCO:** The global guardian of «Ethics and Human Rights.» With 193 adopting states, it provides the most universally accepted vocabulary for ethical AI, focusing heavily on human dignity and cultural diversity. 

- **ITU/ ISO-IEC:** The technical anchors.



Tier 2: The Regulatory Anchor (Hard Law)

- **European Union (EU AI Act):** The only framework currently establishing **binding, mandatory obligations** with extraterritorial reach. It acts as the “Brussels Effect” benchmark—Egyptian companies wishing to export software to Europe will likely need to comply with these standards, regardless of the Egyptian national law. 

Tier 3: Strategic Regional Alliances (Geopolitics & Sovereignty)

Egypt holds a unique geopolitical position, being a member of all the following critical blocs. These frameworks offer Egypt avenues for “Sovereignty-First” governance:

- **African Union (AU):** Focuses on «Africa-centered» ecosystems, emphasizing the preservation of African languages/data and preventing digital colonization. It is voluntary but highly strategic for Egypt’s role as a regional leader. 

- **League of Arab States / AICTO:** Focuses on distinct cultural ethics, conflict resolution, and digital sovereignty. 

- **BRICS:** Represents the «Global South» counter-narrative, focusing on reducing technological dependency on the West and asserting control over national data. 

3.2 Regional & international Lever - Comparative Analysis Matrix

The following table contrasts the key dimensions of 8 selected frameworks to highlight where divergence occurs.

Dimension	EU AI Act	OECD / G20 / G7	UNESCO	AU / Arab League / BRICS
Scope	Risk-based (Unacceptable vs. High Risk)	Broad / Economic Sectors	Broad / Education, Science, Culture	Development Sectors (Agri, Health, Infrastructure)
Legal Status	Mandatory (Regulation)	Voluntary (Soft Law/Political Commitment)	Voluntary (Recommendation)	Voluntary (Cooperation/ Strategy)
Primary Philosophy	Market Safety & Fundamental Rights	Economic Growth & Trustworthy Innovation	Human Rights & Ethical Living	Development, Sovereignty & Capacity Building
Key Mechanism	Conformity Assessments, Fines, Market Surveillance	Policy Observatories, Principles, Information Exchange	Readiness Assessment Methodology (RAM), Impact Assessments	Capacity Building, Infrastructure Investment, Data Localization

3.3 The “Global South” Perspective

While the OECD and EU frameworks provide robust models for interoperability, safety and human rights, research indicates they often overlook constraints specific to developing nations—gaps that the AU, BRICS and other frameworks aim to address.

1. The Data Representation Gap:

Global models (OECD/EU) assume the existence of representative data. The AU and Arab frameworks explicitly highlight the risk of “cultural erasure” due to the lack of African/Arabic datasets and the dominance of Western Foundation Models.

2. The Infrastructure Gap:

Western frameworks focus on regulating the technology. The AU, BRICS, and Islamic Organization (OIC) frameworks focus heavily on building before regulating—emphasizing infrastructure, computing power, and talent pipelines as prerequisites to regulation.

3. The Implementation Gap:

The EU model requires massive institutional capacity (Notified Bodies, enforcement agencies). The ASEAN and African models suggest a “gradual” approach, recognizing that strict immediate enforcement may stifle local startups or overwhelm national regulators.

The Compliance Divide Map: Geopolitical Split

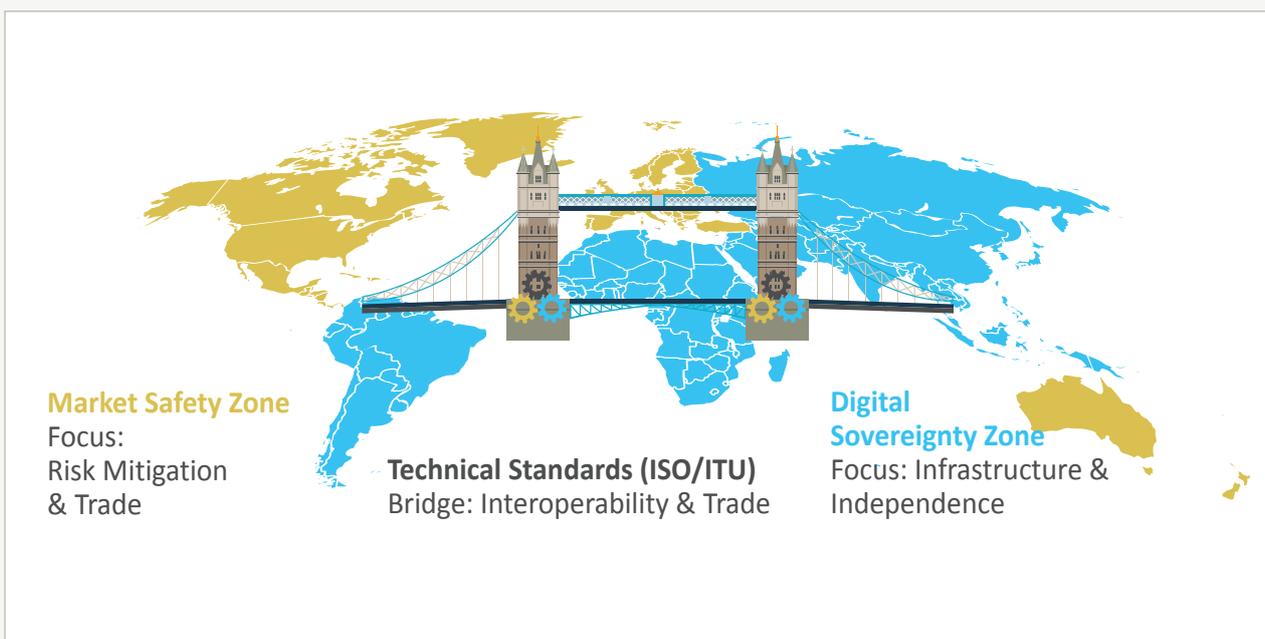


Figure 5: The compliance Divide Map

3.4 Strategic Implications for the Egyptian Framework

Based on the comparative analysis, Egypt should not simply “adopt” one single international framework. Instead, the NCAI is advised to pursue a **Multi-Tiered Alignment Strategy**:

1. Align with OECD/EU for “Interoperability & Trade.”

- **Why:** To ensure Egyptian AI products remain exportable to Europe and the GCC.
- **Action:** Adopt the **OECD’s definitions of AI** and the **Risk-Based Classification** model (e.g., distinguishing High Risk from Low Risk) used by the EU. This creates a «common language» with global investors.

2. Align with AU/Arab League/BRICS for “Sovereignty & Priorities.”

- **Why:** To protect national security, cultural values, and data assets.
- **Action:** Incorporate strong **Data Sovereignty** principles in alignment with the BRICS and AU strategies. Egypt should aim to position itself as the «Data Hub» for the Arab and African regions, leveraging these alliances to build local infrastructure rather than just renting foreign compute

3. Align with UNESCO for “Social License.”

- **Why:** To ensure public trust and cultural acceptance.
- **Action:** Utilize UNESCO’s **Readiness Assessment Methodology (RAM)** to benchmark Egypt’s institutional maturity. The ethical framework should resonate with the values highlighted in the Riyadh Charter and the Tehran Declaration (OIC), and it should respect local cultural and religious contexts.

4. Align with ISO/IEC & ITU for “Quality Assurance & Compliance.”

- **Why:** To ensure the technical reliability, security, and robustness of AI systems.
- **Action:** adopt ISO/IEC 42001 (AI Management System) and ISO/IEC 27001 (Information Security) as the national benchmarks for AI quality.

3.5 Conclusion

Egypt stands at a crossroads. While the **EU AI Act** serves as the inevitable regulatory reference point for global compliance, the **Arab**, African and **BRICS** frameworks offer the most relevant roadmap for economic development and infrastructure independence. The Egyptian National Framework should be a **hybrid**: “Western-compatible” in its safety standards to facilitate trade, but “Global South-centric” in its investment priorities and data governance to ensure sovereignty.

4 National AI Governance Landscapes

This section presents a high-level synthesis of the national AI governance study, providing a comparative regulatory analysis of **14 countries**. Moving beyond simple listings, the analysis classifies Countries into four distinct **Regulatory Models**: Pro-Innovation/Soft Law, Statutory/Risk-Based, Hybrid/Strategic, and Foundational/Developing.

By identifying emerging global paradigms and their specific relevance to developing markets, this section answers a key question: “What is the current state of AI governance on the national level, and what strategic models are currently available to emerging economies?”

4.1 Landscape Mapping - The Four Classification Models

The National Governance Matrix: Finding the Hybrid Sweet Spot

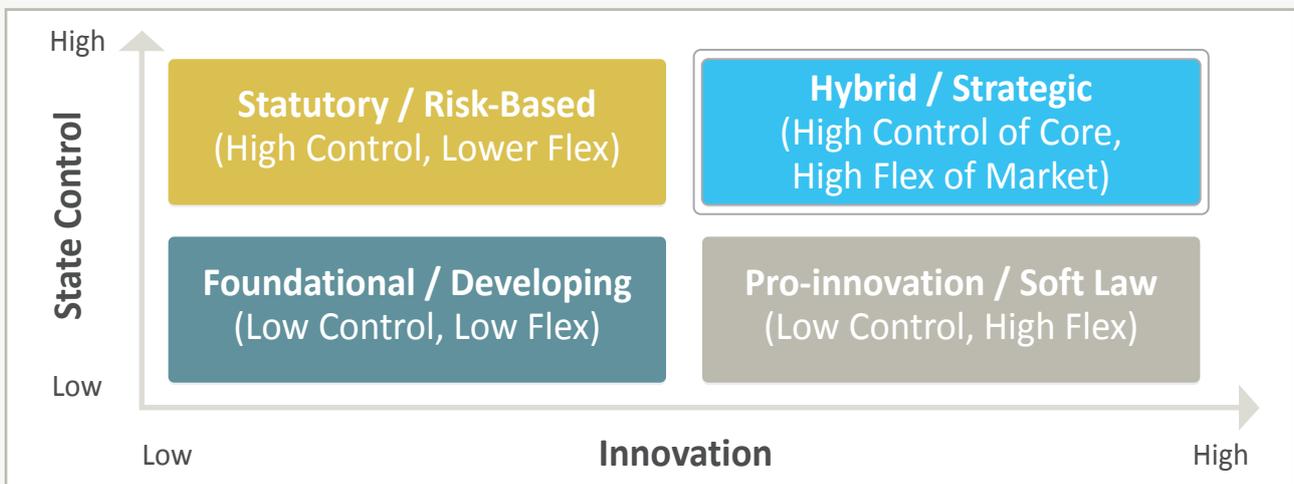


Figure 6: The National Governance Matrix

Model 1: Pro-Innovation / Soft Law

- **Countries:** United States, United Kingdom, Canada, Singapore.
- **Core Philosophy:** Centered on “Market-Led Flexibility,” this philosophy positions the private sector as the primary driver of advancement, with the State acting as a Referee to address specific harms rather than a central architect. These nations explicitly avoid rigid omnibus AI laws to minimize regulatory burdens, prioritizing an open environment that fosters rapid innovation and attracts private investment.
- **Mechanism:** Governance is “decentralized.” Instead of a new AI regulator, existing sector bodies (e.g., finance, healthcare regulators) issue guidance.
- **State as Referee,** the government steps back to let the private sector lead innovation. It acts as an impartial arbiter that only intervenes “ex-post” (after the fact) to penalize specific harms or enforce fair play, rather than dictating how technology should be built.
- **Motto:** “Play the game, we will blow the whistle if you foul.”
- **Key Characteristic:** Reliance on voluntary “soft law” and industry collaboration (e.g., NIST AI RMF, UK Safety Institute, Voluntary Code of Conduct for GenAI, AI Verify Foundation) rather than penalties.

Model 2: Statutory / Risk-Based

- **Countries:** Finland (EU), China, South Korea, Brazil.
- **Core Philosophy:** Centered on “Protective Oversight,” this philosophy views the risks AI poses to fundamental rights, safety, and societal stability as systemic, requiring the State to act as a Guardian rather than just a referee. These countries prioritize legal certainty and public trust above the speed of adoption, mandating binding, horizontal legislation to establish a strict safety baseline that preemptively prohibits harmful applications and rigorously controls high-risk use cases.
- **Mechanism:** A “Risk-Based” methodology that categorizes AI systems into tiers (e.g., Unacceptable, High, Limited risk). High-risk systems face strict mandatory obligations.
- **State as Guardian:** The government acts as a protector of fundamental rights and safety. It enforces strict “ex-ante” (before the fact) rules and conformity assessments to prevent dangerous AI from entering the market, prioritizing public safety over speed.
- **Motto:** “Safety first; prove it is safe before you sell it.”
- **Key Characteristic:** Centralized enforcement with significant penalties for non-compliance, often heavily influenced by or directly adopting the EU AI Act model.

Model 3: Hybrid / Strategic

- **Countries:** Japan, India, Saudi Arabia (KSA), UAE.
- **Core Philosophy:** Centered on “State-Led Strategic Ambition,” this philosophy positions the State as an Architect rather than a passive observer, treating AI governance as a strategic lever for national transformation and sovereignty. These nations aim to become global AI hubs by actively directing the ecosystem, utilizing governance to drive economic diversification and build sovereign capacity while maintaining strategic state control.
- **Mechanism:** A blend of “soft law” guidelines for the private sector to encourage investment, supported by specific mandatory laws for data (Personal Data Protection Law / Digital Personal Data Protection) and government projects.
- **State as Architect:** The government actively designs and builds the ecosystem. It does not just regulate; it funds and owns the critical infrastructure (Sovereign Clouds, National Models) and directs the market toward specific national economic goals.
- **Motto:** “We will build the foundation and direct where the industry goes.”
- **Key Characteristic:** Highly adaptable (“Agile Governance”). They use regulatory sandboxes and “techno-legal” tools (such as digital public infrastructure in India) rather than a single, static AI law.

Model 4: Foundational / Developing

- **Countries:** South Africa, Kenya.
- **Core Philosophy:** Focuses on building the necessary ecosystem (infrastructure, data, skills) while establishing an ethical baseline.
- **Mechanism:** Reliance on high-level policy frameworks and roadmaps rather than enforceable AI statutes.
- **State as Cultivator:** the government focuses on capacity-building. Its primary role is to create the necessary conditions for AI to grow (infrastructure, data, skills) and establish ethical baselines, avoiding premature regulation that might kill the nascent industry.
- **Motto:** “Prepare the soil (infrastructure/skills) so innovation can take root.”
- **Key Characteristic:** Governance is currently achieved through existing data protection laws (e.g., POPIA in South Africa) while dedicated AI legislation is still in the roadmap phase.

4.2 National level - Consolidated Comparative Matrix

The following table contrasts the key dimensions of the researched frameworks to highlight where they diverge.

Country	Domain	Scope	Legal Nature	Regulatory Approach	Methodology	Risk Mgmt. Method	Enforcement & Compliance
Brazil	Both	Legal / Rights-based	Mandatory (Proposed)	Statutory / Binding	Risk-Based	Risk-Tiered (Excessive/ High)	Central Authority Audits
Canada	Split (Public/Private)	Operational (Public) / Policy (Private)	Mandatory (Public) / Voluntary (Private)	Directive (Public) / Voluntary Code	Risk-Based	Risk-Tiered (Public) / Process (Private)	Management Oversight
China	Both	Technical (Filings)	Mandatory	Statutory / State-led	Risk-Based (Security)	Risk-Tiered / Security Assessment	Admin Filings & Security Reviews
Finland (EU)	Both	Legal & Operational	Binding (EU Act)	Statutory / Binding	Risk-Based	Risk-Tiered (EU Model)	Formal Certification & Penalties
India	Both	Principles + “Techno-legal”	Hybrid (Advisory + Data Law)	Principles + Sectoral	Risk-Based (Proportionality)	Process-Based (Lifecycle)	Sectoral Regulators

Country	Domain	Scope	Legal Nature	Regulatory Approach	Methodology	Risk Mgmt. Method	Enforcement & Compliance
Japan	Private Focus	Operational Guidance	Voluntary (Soft Law)	Agile / Innovation-first	Principles-Based	Process-Based (Lifecycle)	Reputational / Voluntary
Kenya	Both	Policy + Technical Code	Hybrid (Voluntary + Binding Data)	Voluntary Standards	Risk-Based	Process-Based (NIST/ ISO)	Sector Regulators (Limited)
KSA	Both	Strategic + Sectoral	Hybrid (Soft + Binding Data)	Soft Regulation + Sandboxes	Principles-Based	Process-Based (ISO 42001)	Centralized Oversight (SDAIA)
Singapore	Private Focus	Operational Governance	Voluntary (Soft Law)	Light-touch / Agile	Principles-Based	Process-Based (Internal)	Voluntary / Market-driven
South Africa	Both	High-level Policy	Voluntary (Policy) + Binding (Data)	Voluntary Guidance	Principles-Based	Process-Based	None Specific (Data Law Only)
South Korea	Both	Legal & Operational	Mandatory	Statutory / Binding	Risk-Based	Risk-Tiered	Statutory Penalties
UAE	Both	Strategic + Sectoral	Hybrid (Data Law + Voluntary)	Agile / Sandboxes	Principles-Based	Process-Based	Existing Regulators
United Kingdom	Both	Principles applied vertically	Voluntary	Sector-led / non-prescriptive	Principles-Based	Process-Based (Regulator discretion)	Existing Regulators / Reporting
United States	Both	Technical Risk Mgmt.	Voluntary	Risk-based / non-prescriptive	Risk-Based	Process-Based (NIST RMF)	Existing Agencies (FTC/ DOJ)

A Glossary list provides clear definitions for each data point in the Consolidated Comparative Matrix.

4.3 Key Areas of Global Convergence and Divergence

This section provides a **descriptive synthesis** of the global AI governance landscape. Its goal is to organize the regulatory data from the 14 surveyed countries into clear, observable patterns. By mapping where nations align and where they fundamentally split, this analysis answers the critical question: Where does the global consensus lie, and what distinct strategic paths are available to policymakers?

A. Areas of Convergence (The “Global Consensus”)

Regardless of their legal model (Soft Law vs. Statutory), all 14 countries have aligned on the following pillars:

1. Adoption of Technical Standards (The “Common Language”): There is a near-universal reliance on international technical standards to operationalize governance. The ISO/IEC 42001 (AI Management System) and NIST AI Risk Management Framework (RMF) are cited as key compliance tools by diverse nations, including the US, India, Kenya, Saudi Arabia, and Japan. This indicates that while *laws* differ, the engineering practices for compliance are harmonizing globally.

2. The “Risk-Based” Model: Every surveyed Country accepts that “not all AI is equal.

- Statutory regimes (EU/Finland, Brazil, South Korea) codify this into rigid “Risk Tiers” (e.g., Prohibited, High, Limited).
- Soft Law regimes (US, UK, Singapore) apply it through context-specific assessments (e.g., NIST’s “Map, Measure, Manage” functions).
- Convergence Point: Governance intensity always scales with the potential for harm.

3. Generative AI as a Trigger for Action: The rise of Generative AI has forced every Country to issue specific, rapid-response guidance, bypassing their standard legislative timelines. This is seen in China’s “Interim Measures”, Singapore’s “GenAI Framework”, the UK’s safety testing, and Canada’s “Voluntary Code”.

4. Ethical Principles Alignment (OECD/UNESCO/ Council of Europe): The foundational values—Transparency, Fairness, Accountability, and Human-Centricity—are identical across the board, stemming from the OECD AI Principles adopted by Japan, South Africa, Canada, and the UK.

B. Areas of Divergence (The “Strategic Splits”)

Countries diverge sharply in their views on the role of the state and the mechanisms of enforcement.

1. The “Hard Law” vs. “Soft Law” Divide:

- **Statutory Binding Rules:** Finland (EU), Brazil, and China impose direct legal obligations with financial penalties for non-compliance.
- **Voluntary “Soft Law”:** The US, UK, Japan, and Singapore explicitly avoid new laws, relying instead on voluntary adoption, market reputation, or “quasi-legal” expectations from regulators.
- **The Split:** The former prioritizes Rights & Safety; the latter prioritizes Speed & Innovation.

2. Centralization vs. Decentralization:

- **Decentralized (Sector-Led):** The UK and US reject a central “AI Regulator,” empowering existing bod(ies) (e.g., Finance or Health regulators) to police their own sectors.
- **Centralized (State-Led):** Saudi Arabia (SDAIA), the UAE (AI Council), and China (CAC) have established powerful central authorities that orchestrate the entire national agenda.

3. Definition of “High Risk”:

- **EU/Brazil Model:** “High Risk” is defined by a rigid, pre-determined list of sectors (e.g., Biometrics, Critical Infrastructure, Education).
- **China Model:** “High Risk” is defined by the ability to mobilize public opinion or disrupt social order.
- **US/UK Model:** “High Risk” is defined contextually by the deploying organization or sector regulator, not by a fixed government list.

4. Enforcement Philosophy:

- **Ex-Ante (Permission-First):** China requires security assessments and filings before a product can be launched.
- **Ex-Post (Harms-Based):** The UK and US typically intervene only after a harm has occurred (e.g., a discrimination lawsuit or consumer complaint).
- **Agile (Sandboxing):** The UAE, KSA, and Singapore focus on “Regulatory Sandboxes” where the government co-develops compliance with the company in real-time.

4.4 Critical Comparative Insights.

Moving beyond the descriptive landscape, this section offers an **analytical interpretation** of the global trends. The goal is to extract the “hidden gems”—the strategic lessons and evolutionary patterns that are not immediately visible in the raw data. Rather than simply comparing laws, this analysis explores the implications of those choices to answer the strategic question: What can the evolution of these global frameworks teach us about designing a successful regime for an emerging ecosystem?

Analysis of the 14 frameworks reveals four macro-trends that define the current global governance environment.

Insight A: The “Soft Law” Pipeline (Regulation is an Evolution)

Contrary to the belief that countries must immediately enact comprehensive laws, innovation hubs like Japan, Singapore, and the UAE utilize a phased lifecycle. They begin with “**Soft Law**” (guidelines, principles, voluntary codes) to build ecosystem maturity and trust. Only once the technology—and the risks—are well understood do they consider transitioning to “Hard Law” (statutes).

Key Takeaway: Premature rigid legislation can lock in obsolete rules. Starting with “Soft law” offers the speed and adaptability required for a nascent AI ecosystem to mature before facing strict regulation.

Insight B: The “Hybrid” Sweet Spot for Emerging Economies

A distinct pattern appears among high-growth emerging economies (India, KSA, UAE). They reject the binary choice between the “US Model” (laissez z-faire) and the “EU Model” (strict regulation). Instead, they adopt a **Hybrid Strategy**:

Pro-Innovation Layer: Flexible guidelines and sandboxes for private sector growth.

Safety Layer: Strict, mandatory rules for government data and specific high-stakes domains (like national security or biometrics), often leveraging existing Data Protection Laws (PDPL/DPDP) as the enforcement hook.

Key Takeaway: The data indicate that high-growth economies have avoided the binary choice between safety and growth by securing the “state core” with hard law while leaving the “market periphery” flexible to attract foreign investment.

Insight C: Standardization as the “Global Passport”

Regardless of a country’s legal stance, there is a near-universal convergence on technical standards. The **NIST AI Risk Management Framework (RMF)** and **ISO/IEC 42001** have become the *de facto* global currency for AI governance. Countries like Kenya, India, and Japan use these standards to ensure their local companies remain export-ready and interoperable with international markets (EU/US) without having to harmonize their entire legal systems.

Key Takeaway: Adopting global technical standards (ISO/NIST) creates an immediate “trade lane” for local AI exports, effectively bypassing the need for complex international treaties to ensure market access.

Insight D: Decentralized Enforcement is the Norm

Most “Pro-Innovation” countries (UK, US, Canada, Japan) do **not** create a single, powerful “AI Regulator.” Instead, they empower **existing sector regulators** (e.g., Central Banks, Health Ministries) to enforce AI principles. This ensures that rules are context-specific—AI in banking is regulated differently than AI in healthcare—avoiding the bottleneck of a single bureaucratic entity.

Key Takeaway: Utilizing existing sector regulators is faster and more precise than building a new AI agency from scratch, as these bodies already possess the domain expertise required to assess specific risks.

4.5 Inherent Structural Challenges

This section serves as the report’s critical risk assessment. Its goal is to move beyond the theoretical benefits of each governance archetype and instead evaluate their inherent structural trade-offs. By identifying the specific “traps” embedded within the Pro-Innovation, Statutory, Hybrid, and Foundational models, this analysis answers the fundamental design question: What are the hidden structural defects in each global model, and why might they pose specific risks to an emerging ecosystem if adopted without adaptation?

Governance Model	Primary Focus	State Role	The Structural Defect (The “Trap”)	Risk for Emerging Ecosystems
Pro-Innovation	Speed & Flexibility	State as Referee:	Regulatory Fragmentation: Relies on a patchwork of existing regulators and voluntary ethics, leading to enforcement gaps.	The “Vacuum” Trap: Without strong, mature institutions to enforce “soft” rules, the market risks becoming a “wild west,” exposing citizens to harm without recourse.
Statutory	Safety & Rights	State as Guardian	Rigidity & Cost: Binding legislation imposes high compliance costs (auditing, documentation) and requires massive state enforcement capacity.	The “Bureaucracy” Trap: Strict “paper laws” may stifle local startups that cannot afford compliance, inadvertently handing market dominance to large foreign incumbents.
Hybrid / Strategic	State Capacity	State as Architect	Talent Dependency: Success depends heavily on the government’s ability to attract rare experts to design and run the central “AI Offices” and to build infrastructure.	The “Capacity” Trap: If the state fails to build the physical infrastructure (compute/data) due to the talent gap, the physical infrastructure promised in the strategy is never actually built, leaving the country with just “paper strategies.”
Foundational	Ecosystem Building	State as Cultivator	Implementation Gap: Governance relies on high-level policies without binding mechanisms or dedicated bodies.	The “Stagnation” Trap: Without enforceable rules or clear ownership, the country remains a passive consumer of AI, and global tech giants may ignore local non-binding policies.

The table above illustrates that the Statutory model may hinder early-stage innovation, while the Pro-Innovation model can create a regulatory gap. In contrast, the Hybrid/Strategic model presents the most promising solution. Its main drawback, Talent Dependency, is an execution challenge, whereas the other models face structural challenges.

4.6 Conclusion

Based on the comprehensive comparative analysis of the 14 countries, here is the summary of the findings on the national level:

1. Emergence of Four Distinct Governance Models

- **Regulatory Archetypes:** The global landscape is not uniform but has fractured into four primary governance models:
- **Pro-Innovation / Soft Law:** Prioritizes market flexibility and sector-specific oversight (e.g., UK, US, Singapore).
- **Statutory / Risk-Based:** Prioritizes legal certainty and rights through binding, horizontal legislation (e.g., EU/Finland, Brazil).
- **Hybrid / Strategic:** Blends voluntary “soft law” for innovation with targeted “hard law” for data and security, often driven by state-led economic strategies (e.g., Saudi Arabia, UAE, India).
- **Foundational / Developing:** Focuses on building ecosystem capacity and ethical baselines while relying on existing data laws (e.g., Kenya, South Africa).

2. The “Hybrid” Shift in Emerging Economies

- **Techno-Legal Approach:** High-growth economies (India, KSA, UAE) are rejecting the binary choice between “laissez-faire” and “strict regulation.” Instead, they are adopting “**Strategic Hybrids**” that combine:
 - **Soft Law:** Flexible guidelines to attract private sector investment and R&D.
 - **Hard Law:** Strict, mandatory rules for sovereign data protection and digital infrastructure to maintain state control.
- **State as Architect:** Unlike the “State as Referee” model in the West, these governments actively build the ecosystem (sovereign clouds, foundational models) while regulating it.

3. Global Convergence on Technical Standards

- **De Facto Interoperability:** Despite diverging legal systems (Common Law vs. Civil Law), there is a near-universal convergence on technical risk management standards.
- **The “Common Language”:** Frameworks like **ISO/IEC 42001** and the **NIST AI Risk Management Framework (RMF)** are being adopted globally (from the US to Kenya and Japan) to operationalize governance, creating a trade lane for interoperability regardless of national statutes.

4. Tailoring Governance to National Imperatives

- **Context-Specific Priorities:** Successful frameworks are not “copy-paste” solutions but are engineered to solve specific national challenges:
- **Brazil:** Structures its law to combat deep-seated **social inequality** and discrimination.
- **China:** Focuses on **state security**, social stability, and information control.
- **Saudi Arabia & UAE:** Use governance as a strategic lever for **economic diversification** (e.g., Vision 2030) to transition away from oil dependence.

5. The “Soft Law” Pipeline

- **Evolutionary Regulation:** Data from mature hubs (Singapore, UK) suggests that regulation is an evolution, not an event. Most jurisdictions start with “**Soft Law**” (voluntary codes, principles) to build ecosystem maturity and trust, reserving “**Hard Law**” for mature, high-stakes risks later. Premature rigid legislation is seen as a risk that can lock in obsolete rules.

6. Decentralization vs. Centralization

- **Enforcement Divide:** There is a sharp split in how rules are enforced:
- **Decentralized:** Pro-innovation nations (UK, US) empower **existing sector regulators** (e.g., Finance, Health) to enforce AI rules, avoiding a bottleneck.
- **Centralized:** Strategic nations (China, KSA) establish powerful **central authorities** (e.g., CAC, SDAIA) to orchestrate the entire national AI agenda.

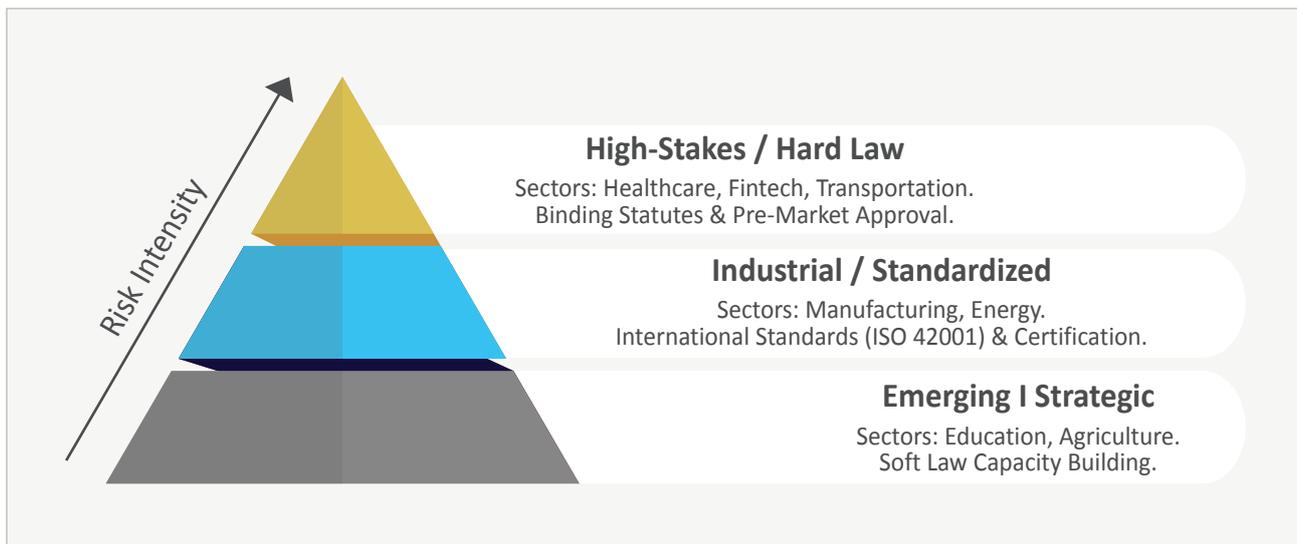
5 Sectoral AI Governance Landscapes

This section distills comparative sectoral data into actionable intelligence to determine emerging global governance models. The analysis reveals that regulation scales directly with risk, classifying industries into three distinct models: **High-Stakes** (e.g., Healthcare), governed by binding statutes; Industrial (e.g., Manufacturing), governed by international standards; and Emerging (e.g., Agriculture), governed by strategic soft law.

Two strategic shifts define this landscape. First, a “Horizontal Shift” driven by the EU AI Act means specific high-risk functions—such as hiring—trigger strict mandates regardless of the sector label. Second, international certification (e.g., ISO/IEC 42001) has become a de facto “global passport” for industrial supply chains, often superseding domestic national laws for market access.

5.1 Landscape Mapping- Three Classification Models.

The Sectoral Risk Pyramid: A Three-Tiered Reality



Model 1: High-Stakes / Hard Law

- **Sectors:** Healthcare, Transportation, Fintech.
- **Core Philosophy:** Centered on “**Harm Prevention**,” this philosophy views the risks AI poses to life and financial stability as systemic. It prioritizes safety and accountability over speed, mandating strict ex-ante (pre-market) conformity.
- **Mechanism:** Governance is “statutory.” It relies on binding administrative rules, such as the Food and Drug Administration (FDA) “Total Product Lifecycle” or the United Nations Economic Commission for Europe (UNECE) binding vehicle regulations.
- **Key Characteristic:** Centralized enforcement with significant penalties. For example, the EU AI Act classifies these sectors as “High Risk,” requiring rigorous conformity assessments.

Model 2: Industrial / Standardized

- **Sectors:** Manufacturing, Energy.
- **Core Philosophy:** Centered on “**Reliability & Efficiency,**” this philosophy positions technical robustness as the primary driver. The State acts as a standard-setter to protect critical infrastructure.
- **Mechanism:** Governance is “Standards-Led.” It relies on voluntary but de facto mandatory international standards like ISO/IEC 42001 (Management) and ISO/IEC 27001 (Cybersecurity).
- **Key Characteristic:** Reliance on third-party certification and management systems rather than direct government policing of algorithms.

Model 3: Emerging / Strategic

- **Sectors:** Agriculture, Education.
- **Core Philosophy:** Centered on “**Capacity Building & Equity,**” this philosophy focuses on using AI to solve developmental challenges. Regulation is currently “soft” to encourage adoption.
- **Mechanism:** Governance is “Strategic.” It relies on policy guidance (UNESCO, OECD-FAO) and national roadmaps (e.g., India’s MahaAgri-AI).
- **Key Characteristic:** Governance is primarily through existing non-binding frameworks, though the EU AI Act is beginning to intrude with specific high-risk classifications for labor and grading.

5.2 Sectoral Level - Consolidated Comparative Matrix

The following table compares the key dimensions of the researched frameworks to highlight where they diverge.

Sector	Model	Regulatory Focus	Legal Nature	Regulatory Approach	Risk Mgmt. Method	Enforcement
Healthcare	High-Stakes	Safety & Ethics	Mandatory ((Binding	Statutory / Lifecycle	Risk-Tiered (EU/ (FDA	Pre-Market Approval
Transportation	High-Stakes	Safety & Liability	Mandatory ((Binding	International Regs	Risk-Tiered / Black Box	Type Approval / Homologation
Fintech	High-Stakes	Fairness / Explainability	Mandatory (Existing (Law	Interagency Guidance	Process-Based ((Adverse Action	Existing Agencies (CFPB/ (Central Banks
Manufacturing	Industrial	Quality & Safety	Voluntary ((Standards	Industry-Led	Process-Based ((ISO 42001	Third-Party Certification
Energy	Industrial	Security & Efficiency	Hybrid (Standards + (Law	Sector-Specific	Risk-Based ((Cybersecurity	Critical Infra Protection
Education	Emerging	Rights & Literacy	Voluntary ((Soft Law	Policy Guidance	Principles-Based ((Human-Centric	Soft / EU High-Risk Exceptions
Agriculture	Emerging	Supply Chain / Labor	Voluntary ((Soft Law	Strategic Roadmaps	Principles-Based ((Sustainability	Soft / EU High-Risk Exceptions

A Glossary list provides clear definitions for each data point in the Consolidated Comparative Matrix.

5.3 Key Areas of Global Convergence and Divergence

This section provides a descriptive synthesis of the global sectoral landscape. By mapping where sectors align and where they fundamentally split, this analysis answers the critical question: Where does the global consensus lie across industries?

A. Areas of Convergence (The “Global Consensus”)

Regardless of the sector, all domains have aligned on the following pillars:

- 1. Adoption of Technical Standards (The “Common Language”):** There is a near-universal reliance on international technical standards to operationalize governance. **ISO/IEC 42001** and **ISO/IEC 27001** are cited as key compliance tools in Manufacturing, Energy, and Healthcare.

2. The “High-Risk” Mental Model: Every sector accepts that strictness must scale with risk. The **EU AI Act** has standardized this by creating a “High-Risk” category that applies horizontally, covering medical devices, safety components in cars/machinery, and credit scoring alike.

3. Transparency & Explainability: Whether it is “Adverse Action” notices in Fintech ²¹or “Intelligibility” in healthcare, there is global convergence that AI decisions must be explainable to humans.

B. Areas of Divergence (The “Strategic Splits”)

The sectors diverge sharply in their views on the mechanism of enforcement.

1. “Agile” vs. “Pre-Market” Approval:

- **Pre-Market:** The EU and China require strict testing *before* deployment in Healthcare and Transport.
- **Agile:** The US FDA and UK MHRA are moving toward “Lifecycle” governance (Predetermined Change Control Plan (PCCP)), allowing models to update post-deployment without re-certification.

2. Horizontal vs. Vertical Regulation:

- **Vertical:** Fintech and Transportation rely heavily on existing sector-specific bodies (Central Banks, UNECE) to interpret rules.
- **Horizontal:** The EU AI Act imposes a new layer of rules that applies across all sectors, creating a split between regions that regulate “AI” (EU) and regions that regulate “AI in X” (US/UK).

5.4 Critical Comparative Insights

This section offers an analytical interpretation of the sectoral trends. The goal is to extract the “hidden gems”—the strategic lessons and evolutionary patterns that are not immediately visible in the raw data.

■ **Insight A:** The “Hidden” Regulator (Scope Creep): Organizations in “Emerging” sectors like Agriculture and Education often underestimate their regulatory exposure. A key insight is that regulation is triggered by function, not sector. An agricultural AI used for workforce management is legally “High-Risk” under the EU AI Act, subjecting it to the same strictness as a medical device.

■ **Insight B:** Standards as the “Real” Law: In industrial sectors (Manufacturing, Energy), technical standards (ISO) effectively function as law. While laws provide the “what” (be safe), standards like ISO 42001 provide the “how.” Compliance with these is the primary barrier to entry for global supply chains.

■ **Insight C:** The Gap between Static Regulation and Agile AI: A critical tension exists in safety-critical sectors. Traditional regulation (e.g., Chinese clinical trials 29) treats software as a fixed product. However, the emerging “Best Practice” (US FDA PCCP 30) treats it as an evolving service, creating a strategic split in how nations manage AI innovation.

5.5 Inherent Structural Challenges

This section serves as the report’s critical risk assessment. Its goal is to evaluate the inherent structural trade-offs within the governance models of each sector cluster.

Governance Model	Primary Focus	The Structural Defect (The “Trap”)	Risk for Emerging Ecosystems
High-Stakes / Hard Law	Safety & Liability	Rigidity vs. Update Speed: Strict pre-market approval can freeze AI models, preventing them from learning and improving.	The “Obsolescence” Trap: Regulators may force hospitals/banks to use outdated AI because the “safer” updated version hasn’t passed a 12-month review.
Industrial / Standardized	Reliability	Certification Cost: Achieving ISO 42001/27001 certification is expensive and document-heavy.	The “Barrier” Trap: Small manufacturers may be locked out of global supply chains, ceding the market to large incumbents who can afford certification.
Emerging / Strategic	Equity & Growth	Lack of Enforceability: Reliance on “Ethical Principles” without penalties leads to non-compliance.	The “Ethics Washing” Trap: Without binding rules, educational or agricultural AI may claim to be “fair” while secretly monetizing vulnerable user data.

The table above shows that the High-Stakes model offers safety but risks obsolescence. While the Emerging model offers growth, it risks exploitation. The Industrial model (Standards-based) provides the most balanced path for operational governance, as it scales rigor with complexity.

5.6 Conclusion

The analysis confirms that global governance has matured from generic principles into a **“Three-Tiered Reality,”** in which compliance is determined by risk rather than industry labels. **High-Stakes sectors** (Healthcare, Finance) now face binding **“Hard Law”** mandates, while **Industrial sectors** (Manufacturing, Energy) rely on **International Standards** (ISO/IEC) as a prerequisite for global market access. Meanwhile, **emerging sectors** (Agriculture, Education) remain in a strategic **“Soft Law”** phase to foster adoption. Ultimately, organizations must now navigate these concurrent regimes, determining their regulatory obligations based on the specific function of their AI tools rather than their broader sector category.

6 References and Appendices

This section offers a comprehensive list of all primary source documents, academic articles, and other resources cited in the report. Appendices will include a glossary of key terms and a complete list of the 37 frameworks analyzed.

6.1 References

This section lists the primary source documents and key reports that informed this analysis.

A. Regional & International Frameworks

OECD



- OECD AI Principles official overview: “AI principles | OECD.”

<https://www.oecd.org/en/topics/sub-issues/ai-principles>

- 2024 update press release: “OECD updates AI Principles to stay abreast of rapid technological developments.”

<https://www.oecd.org/en/about/news/press-releases/2024/05/oecd-updates-ai-principles-to-stay-abreast-of-rapid-technological-developments.html>

- 2019 Recommendation full text (PDF) — referred to in various sources.

https://nangs.org/analytics/oecd-oecd-principles-on-artificial-intelligence-may-2019-eng-pdf?utm_source=chatgpt.com

- 2024 OECD report “Governing with Artificial Intelligence: Are Governments Ready?”

https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/governing-with-artificial-intelligence_f0e316f5/26324bc2-en.pdf?utm_source=chatgpt.com

- 2024 regional report e.g. “OECD Artificial Intelligence — Review of Egypt”

https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/05/oecd-artificial-intelligence-review-of-egypt_3c437131/2a282726-en.pdf?utm_source=chatgpt.com

- OECD background page on AI-governance work and AIGO: “About background” page on OECD.AI

<https://oecd.ai/en/about-background>



UNESCO

- UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence. UNESCO.

<https://www.unesco.org/en/legal-affairs/recommendation-ethics-artificial-intelligence>

- UNESCO. (2023). Ethical Impact Assessment: A Tool of the Recommendation on the Ethics of Artificial Intelligence. UNESCO.

<https://www.unesco.org/en/articles/ethical-impact-assessment-tool-recommendation-ethics-artificial-intelligence>

- UNESCO. (2023). Readiness Assessment Methodology: A Tool of the Recommendation on the Ethics of Artificial Intelligence. UNESCO.

<https://www.unesco.org/en/articles/readiness-assessment-methodology-tool-recommendation-ethics-artificial-intelligence>

- UNESCO. (n.d.). Ethics of Artificial Intelligence. UNESCO.

<https://www.unesco.org/en/articles/ethics-ai>

- UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence [PDF]. Integrated Monitoring (IM) Portal.

https://www.im-portal.org/system/files/content/resource/files/main/2021_Recommendation_ethics_AI_UNESCO.pdf

- UNESCO. (n.d.). التوصية بشأن أخلاقيات الذكاء الاصطناعي.

<https://www.unesco.org/ar/artificial-intelligence/recommendation-ethics>

Hiroshima AI Process



- G7. Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI Systems. 30 Oct. 2023,

<https://g7g20-documents.org/database/document/2023-g7-japan-leaders-leaders-annex-hiroshima-process-international-guiding-principles-for-organizations-developing-advanced-ai-system>.

■ G7. Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems. 30 Oct. 2023,

<https://g7.utoronto.ca/summit/2023hiroshima/231030-ai-code-of-conduct.html>.

■ G7. G7 Leaders' Statement on the Hiroshima AI Process. 30 Oct. 2023,

https://www.international.gc.ca/world-monde/international_relations-relations_internationales/g7/documents/2023-10-30-ai-hiroshima-ia.aspx.

■ G7. G7 Digital & Tech Ministers' Statement on the Hiroshima AI Process. 7 Sept. 2023,

<https://www.g7.utoronto.ca/ict/2023-statement-2.html>.

■ Organization for Economic Co-operation and Development. OECD launches pilot to monitor application of G7 code of conduct on advanced AI development. 22 July 2024,

<https://www.oecd.org/en/about/news/press-releases/2024/07/oecd-launches-pilot-to-monitor-application-of-g7-code-of-conduct-on-advanced-ai-development.html>.

■ OECD. OECD launches global framework to monitor application of G7 Hiroshima AI Code of Conduct. 7 Feb. 2025,

<https://www.oecd.org/en/about/news/press-releases/2025/02/oecd-launches-global-framework-to-monitor-application-of-g7-hiroshima-ai-code-of-conduct.html>.

■ Italian G7 Presidency. G7 Digital & Tech Working Group Finalizes Reporting Framework for Advanced AI Systems. 23 Dec. 2024,

<https://innovazione.gov.it/notizie/articoli/en/g7-digital-tech-working-group-finalizes-reporting-framework-for-advanced-ai-syste/>.

■ Hogan Lovells. G7 releases Guiding Principles and a voluntary Code of Conduct for AI developers.

<https://www.hoganlovells.com/en/publications/g7-releases-guiding-principles-and-a-voluntary-code-of-conduct-for-ai-developers>.

■ Istituto Affari Internazionali. The G7 and AI Governance: Towards a Deeper and Broader Agenda. 2024,

<https://www.iai.it/sites/default/files/iaip2428.pdf>.

- G7 (Global Partnership on Artificial Intelligence). About GPAI. GPAI, 2020,
<https://gpai.ai/about/>. gpai.ai+1
- OECD. Global Partnership on Artificial Intelligence (GPAI). OECD,
<https://www.oecd.org/en/about/programmes/global-partnership-on-artificial-intelligence.html>. OECD+1
- Organization for Economic Cooperation and Development. “GPAI and OECD unite to advance coordinated international efforts for trustworthy AI.” OECD, 3 July 2024,
<https://www.oecd.org/en/about/news/speech-statements/2024/07/GPAI-and-OECD-unite-to-advance-coordinated-international-efforts-for-trustworthy-AI.html>. OECD
- Global Partnership on Artificial Intelligence. GPAI FAQ. GPAI, Nov. 2021,
<https://www.gpai.ai/about/gpai-faq.pdf>. gpai.ai
- Global Partnership on Artificial Intelligence. GPAI Data Governance Working Group – Work Framework Paper. GPAI, Nov. 2020,
<https://gpai.ai/projects/data-governance/gpai-data-governance-wg-report-november-2020.pdf>. gpai.ai+1
- Global Partnership on Artificial Intelligence. “An Introduction to the Global Partnership on AI’s Work on Innovation and Commercialization.” OECD.AI, 13 Oct. 2020,
<https://oecd.ai/en/wonk/an-introduction-to-the-global-partnership-on-ais-work-on-innovation-and-commercialization.oecd.ai>
- Global Partnership on Artificial Intelligence. The Global Partnership on Artificial Intelligence (GPAI). Wikipedia, 2025,
https://en.wikipedia.org/wiki/Global_Partnership_on_Artificial_Intelligence.

- World Economic Forum. The AI Governance Journey: Development and Opportunities. 2021.

https://www3.weforum.org/docs/WEF_The%20AI_Governance_Journey_Development_and_Opportunities_2021.pdf. World Economic Forum

- World Economic Forum. Empowering AI Leadership: AI CSuite Toolkit. 12 Jan. 2022.

<https://www.weforum.org/publications/empowering-ai-leadership-ai-c-suite-toolkit/>. World Economic Forum+1

- World Economic Forum. “Artificial Intelligence Toolkit Helps Companies Protect Society and Their Business.” 17 Jan. 2020.

<https://www.weforum.org/press/2020/01/artificial-intelligence-toolkit-helps-companies-protect-society-and-their-business/>. World Economic Forum+1

- World Economic Forum. “World Economic Forum Launches New Global Initiative to Advance the Promise of Responsible Artificial Intelligence.” 28 Jan. 2021.

<https://www.weforum.org/press/2021/01/world-economic-forum-launches-new-global-initiative-to-advance-the-promise-of-responsible-artificial-intelligence/>. World Economic Forum+1

- World Economic Forum. “World Economic Forum Launches AI Governance Alliance Focused on Responsible Generative AI.” 15 June 2023.

<https://www.weforum.org/press/2023/06/world-economic-forum-launches-ai-governance-alliance-focused-on-responsible-generative-ai/>. World Economic Forum+1

- World Economic Forum. AI Governance Alliance — Briefing Paper Series. Jan. 2024.

<https://www.weforum.org/publications/ai-governance-alliance-briefing-paper-series/>. World Economic Forum+1

- World Economic Forum. Generative AI Governance: Shaping a Collective Global Future. 2024.

https://www3.weforum.org/docs/WEF_Generative_AI_Governance_2024.pdf. World Economic Forum

- World Economic Forum. “Towards a Strong TrustBased AI Governance Model.” 2023.

<https://www.weforum.org/agenda/2023/05/towards-a-strong-trust-based-ai-governance-model/>

ITU



- International Telecommunication Union. ITU-T Y.3172: Architectural framework for machine learning in future networks including IMT2020. 22 June 2019, <https://www.itu.int/rec/T-REC-Y.3172-201906-P>. ITU+1
- International Telecommunication Union. New ITU standard to introduce Machine Learning into 5G networks. “AI for Good”, 2019, <https://aiforgood.itu.int/new-itu-standard-to-introduce-machine-learning-into-5g-networks/>. AI for Good+1
- International Telecommunication Union. Focus Group on “Artificial Intelligence for Health” (FGAI4H). ITU, <https://www.itu.int/en/ITU-T/focusgroups/ai4h/Pages/default.aspx>. ITU+1
- International Telecommunication Union / World Health Organization. FGAI4H DEL2.1: Mapping of IMDRF essential principles to AI for health software. 2023, https://www.itu.int/dms_pub/itu-t/opb/fg/T-FG-AI4H-2023-4-PDF-E.pdf. ITU
- International Telecommunication Union. International standards for an AI-enabled future. ITU, July 2020, <https://www.itu.int/hub/2020/07/international-standards-for-an-ai-enabled-future/>. ITU+1
- International Telecommunication Union. Artificial Intelligence for Health — AI for Good Global Initiative. ITU, <https://aiforgood.itu.int/artificial-intelligence-for-health/>. AI for Good+1
- International Telecommunication Union. FGAI4H: Clinical evaluation of AI for health. 2023, https://www.itu.int/dms_pub/itu-t/opb/fg/T-FG-AI4H-2023-.3-PDF-E.pdf. ITU
- Aiforgood data base: <https://aiforgood.itu.int/ai-standards-exchange/ai-standards-exchange-database/>

BRICS



- BRICS. AI governance takes center stage as BRICS ministers sign new declaration. CADE – Civil Society Alliances for Digital Empowerment, 29 Apr. 2025,

■ cadeproject.org/updates/ai-governance-takes-center-stage-as-brics-ministers-sign-new-declaration/. CADE

■ BRICS. Artificial Intelligence Governance in BRICS: Cooperation and Development for Social Inclusion. 11 Apr. 2025, brics.br/en/news/articles/artificial-intelligence-governance-in-brics-cooperation-and-development-for-social-inclusion. BRICS Brazil

■ “BRICS Sign Joint Declaration on Artificial Intelligence in Education, Formalize Technical and Vocational Cooperation Alliance.” BRICS Brazil, 10 June 2025, brics.br/en/news/brics-sign-joint-declaration-on-artificial-intelligence-in-education-formalize-technical-and-vocational-cooperation-alliance. BRICS Brazil

■ BRICS. XIV BRICS Summit Beijing Declaration (2022). 2022, bricswomen.com/wp-content/uploads/2024/04/XIV-BRICS-Summit-Beijing-Declaration-2022-1.pdf. Brics Women

■ “BRICS Working Group on Digital Markets Puts Spotlight on AI.” BRICS Competition, 23 Apr. 2025, bricscompetition.org/ournews/brics-working-group-on-digital-markets-puts-spotlight-on-ai. BRICS Competition+1

■ “BRICS Leaders Reaffirm Support for Digital Sovereignty and Inclusive AI Access.” ITWeb, 2025, itweb.co.za/article/brics-leaders-call-for-inclusive-access-to-ai/WnXPv4YW2m7V8XL. ITWeb

■ BRICS. Chair’s Statement of the Meeting of BRICS Foreign Ministers, 29 April 2025. 2025, brics.br/en/documents/2025-04-29_brics-mfa-chairs-statement.pdf. BRICS Brazil

■ “Global AI governance must address needs of all nations — BRICS declaration.” TASS, 6 July 2025, tass.com/world/1986125. TASS

■ Centro Brasileiro de Relações Internacionais (CEBRI). Digital Transformation and Artificial Intelligence (AI) — BRICS Dialogue Paper. 2025, cebri.org/media/documentos/arquivos/BRICS_Dialogue_Papers_VF30.06.pdf.

G20



■ G20. G20 Principles for Responsible Stewardship of Trustworthy Artificial Intelligence. Digital Economy Ministerial Meeting, Tsukuba, Japan, June 2019. G20, 2019.

https://www.g20.org/en/media/Documents/G20_AI_Principles.pdf.

■ G20. G20 Leaders’ Declaration: Bali Summit 2023. G20, 2023.

https://www.g20.org/en/media/Documents/G20_Leaders_Declaration_Bali_2023.pdf.

- G20. G20 Leaders' Declaration: 2024 (India Presidency). G20, 2024.

https://www.g20.org/en/media/Documents/G20_Leaders_Declaration_2024.pdf

- G20. G20 Leaders' Declaration: 2025 (South Africa Presidency). G20, 2025.

https://www.g20.org/en/media/Documents/G20_Leaders_Declaration_2025.pdf

- G20 Digital Economy Working Group. G20 AI, Data Governance, and Innovation for Sustainable Development: Task Force Report 2025. G20, 2025.

<https://www.g20.org/en/digital-economy/ai-task-force-2025.pdf>

- Organization for Economic Co-operation and Development (OECD). OECD Principles on Artificial Intelligence. OECD, 2019.

<https://www.oecd.org/going-digital/ai/principles/>

- United Nations Educational, Scientific and Cultural Organization (UNESCO). Recommendation on the Ethics of Artificial Intelligence. UNESCO, 23 Nov. 2021.

<https://www.unesco.org/en/artificial-intelligence/ethics>

International Network of AI Safety Institutes



- International Network of AI Safety Institutes. Mission Statement. 21 Nov. 2024. International Network of AI Safety Institutes, San Francisco.

- U.S. Department of Commerce and U.S. Department of State. Fact Sheet: Funding Commitments and Technical Focus Areas for International AI Safety Research. 21 Nov. 2024. U.S. Department of Commerce, Washington, D.C.

- International Network of AI Safety Institutes. Joint Statement on Risk Assessments of Advanced AI Systems. 21 Nov. 2024. International Network of AI Safety Institutes, San Francisco.

- Seoul Statement of Intent Toward International Cooperation on AI Safety Science. 21 May 2024. Republic of Korea.

Latin America and Caribbean Regional Council on the Ethics of AI



■ Latin America and Caribbean Regional Council on the Ethics of AI. Regional Initiatives on Ethical AI: Principles and Objectives. 2020–2023. Latin America and Caribbean AI Ethics Network, Regional Consultative Platform.

■ Economic Commission for Latin America and the Caribbean (ECLAC). AI Governance for the Caribbean. ECLAC, Dec. 2023,

<https://www.cepal.org/en/publications/81180-ai-governance-caribbean>.

■ Inter-American Development Bank (IDB). fAIr LAC: Responsible and Widespread Adoption of Artificial Intelligence in Latin America and the Caribbean. IDB, 2020,

<https://publications.iadb.org/en/fair-lac-responsible-and-widespread-adoption-of-artificial-intelligence-in-latin-america-and-the-caribbean>.

■ UNESCO. “CAF and UNESCO Will Create a Council to Review Ethical Criteria for Artificial Intelligence in Latin America and the Caribbean.” UNESCO, 2022,

<https://www.unesco.org/en/articles/caf-and-unesco-will-create-council-review-ethical-criteria-artificial-intelligence-latin-america-and>.

The African Region



■ African Union. Continental Artificial Intelligence Strategy. African Union Executive Council, 18–19 July 2024. African Union, 2024.

■ African Union. “Multistakeholder Consultative Sessions on the Development of a Continental Strategy on Artificial Intelligence (AI).” African Union, 19 Apr. 2024.

■ African Union. “African Ministers Adopt Landmark Continental Artificial Intelligence Strategy, African Digital Compact to drive Africa’s Development and Inclusive Growth.” Press release, 17 June 2024. African Union, 2024.

■ UNESCO. “UNESCO’s support to AU’s Continental AI Framework and Strategy.” UNESCO, 28 Aug. 2024. UNESCO

■ African Union Peace and Security Council. “Communiqué of the 1267th Meeting ... on Artificial Intelligence and its Impact on Peace, Security and Governance in Africa.” 20 Mar. 2025. African Union, 2025.



ASEAN Working Group

- ASEAN. ASEAN Guide on AI Governance and Ethics. 2 Feb. 2024. ASEAN Secretariat.
- ASEAN. Expanded ASEAN Guide on AI Governance and Ethics – Generative AI. Jan. 2025. ASEAN Secretariat.
- Infocomm Media Development Authority (IMDA). “About the ASEAN Working Group on AI Governance (WGAI).” IMDA, 2025,
<https://www.imda.gov.sg/about-imda/international-relations/asean-working-group-on-ai-governance>.
- ASEAN Secretariat. “The Quest Toward Developing an AI Governance in ASEAN.” The ASEAN Magazine, 4 June 2024,
<https://theaseanmagazine.asean.org/article/theaseaneconomiccommunitydigest-thequesttowarddevelopinganaigovernanceinaseaninsightsfromthe11thaseanecomiccommunitydialogue>.
- ASEAN Secretariat. “ASEAN Releases Expanded Guide on AI Governance and Ethics Covering Generative AI.” The Legal Wire, 17 Jan. 2025,
<https://thelegalwire.ai/asean-releases-expanded-guide-on-ai-governance-and-ethics/>



Arab Region

- Arab League. Draft Common Arab AI Strategy. Arab ICT Ministers Working Group, 2025.
- Arab Information & Communication Technologies Organization (AICTO). Arab Ethical Framework for Artificial Intelligence. AICTO, 2025.
- Arab League Educational, Cultural and Scientific Organization (ALECSO). Charter on AI Ethics in Education, Culture, and Science. June 2025,
<https://www.alecso.org/en/charter-ai-ethics>.
- Arab League. “Arab Dialogue Roundtable on Artificial Intelligence in the Arab World: Innovative Applications and Ethical Challenges, Cairo, 2–3 Feb. 2025: Final Statement.” LAS Publications, 2025.

■ Arab League. AI Initiative by the Secretary General of the League of Arab States, Baghdad, 2025.

■ Arab Academy for Science, Technology and Maritime Transport. Annual Arab Forum on Artificial Intelligence Proceedings, New Alamein, Egypt, 27–28 Aug. 2025.

■ UNESCO. Recommendation on the Ethics of Artificial Intelligence. United Nations Educational, Scientific and Cultural Organization, 2021,

<https://unesdoc.unesco.org/ark:/48223/pf0000377897>.

■ United Nations Development Programme (UNDP). Digital for Sustainable Development: Arab Region Partnership Overview. UNDP Regional Hub for Arab States, 2025,

<https://www.arabstates.undp.org/digital-ai>.

Islamic Organization



■ Organization of Islamic Cooperation (OIC). Tehran Declaration: Trustworthy and Ethical Artificial Intelligence for Sustainable Development. OIC 15 Dialogue Platform, Tehran, May 2025.

■ Islamic World Educational, Scientific and Cultural Organization (ICESCO / ISESCO). Riyadh Charter for Artificial Intelligence in the Islamic World. 45th Executive Council Session, Global AI Summit, Riyadh, Sept. 2024.

■ ICESCO / ISESCO. Strategic Framework for AI Governance in Islamic Countries. ICESCO Publications, 2024–2025.

■ Scholarly Analysis: Al-Khater, Faisal, and Zainab Al-Mansour. “Ethical AI and Sharia Principles: Aligning Technology Governance in Islamic Countries.” *Journal of Islamic Ethics and Technology*, vol. 3, no. 2, 2025, pp. 45–68.

■ Scholarly Analysis: Hassan, Omar. “The Riyadh Charter and Tehran Declaration: Voluntary AI Governance in the Islamic World.” *AI & Society Review*, vol. 7, no. 1, 2025, pp. 12–27.

Council of Europe



- Council of Europe. HUDERIA: Risk and Impact Assessment of AI Systems. Council of Europe, 2024,

<https://www.coe.int/en/web/artificial-intelligence/huderia-risk-and-impact-assessment-of-ai-systems>. Accessed 4 Dec. 2025.

- Council of Europe. “AI Risk and Impact Assessment – Launch of the HUDERIA Process.” Council of Europe, 2025,

<https://www.coe.int/en/web/artificial-intelligence/-/ai-risk-and-impact-assessment-launch-of-the-huderia-process>. Accessed 4 Dec. 2025.

- Council of Europe. Brochure on Artificial Intelligence. Council of Europe, 2023,

<https://rm.coe.int/brochure-artificial-intelligence-en-march-2023-print/1680aab8e6>. Accessed 4 Dec. 2025.

- Council of Europe. “HUDERIA: New Tool to Assess the Impact of AI Systems on Human Rights.” Council of Europe, Dec. 2024,

<https://www.coe.int/en/web/portal/-/huderia-new-tool-to-assess-the-impact-of-ai-systems-on-human-rights>. Accessed 4 Dec. 2025.

- Council of the European Union. Artificial Intelligence (AI) Act: Council Gives Final Green Light to the First Worldwide Rules on AI. 21 May 2024,

<https://data.consilium.europa.eu/doc/document/ST-11364-2024-INIT/en/pdf>. Accessed 4 Dec. 2025.

- European Commission. European Artificial Intelligence Act Comes into Force. 1 Aug. 2024,

https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_24_4123/IP_24_4123_EN.pdf. Accessed 4 Dec. 2025.

- Council of Europe. Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law (CETS No. 225). 17 May 2024,

<https://rm.coe.int/brochure-artificial-intelligence-en-march-2023-print/1680aab8e6>. Accessed 4 Dec. 2025.

■ ISO/IEC

ISO/ IEC standards: <https://www.iso.org/standards.html>
HYPERLINK “<https://www.iso.org/standard/42001>”ISO/IEC 42001:2023
HYPERLINK “<https://www.iso.org/standard/27001>”ISO/IEC 27001:2022
The Egyptian Organization for standardization: www.eos.org

■ IEEE

IEEE Portal: HYPERLINK “<http://www.ieee.org>”www.ieee.org

■ UN

GDC: Global Digital Compact; https://www.un.org/global-digital-compact/sites/default/files/2024-/Global%20Digital%20Compact%20-%20English_0.pdf
Global Digital Compact — UN information page <https://www.un.org/global-digital-compact/en>
UNGA AI Resolutions; Resolution 78/265 — “Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development”; <https://digitallibrary.un.org/record/4040897?ln=en>
Resolution 78/311 — “Enhancing international cooperation on capacity-building of artificial intelligence”; <https://digitallibrary.un.org/record/4043244?ln=en>
HYPERLINK “https://www.g20.utoronto.ca/compliance/2023newdelhi-final/07-2023-g20-compliance-final-AI.pdf?utm_source=chatgpt.com”G20 Summit

- European External Action Service. “European Commission Signs Historic Council of Europe Framework Convention on Artificial Intelligence and Human Rights.” EEAS, 5 Sept. 2024,

https://www.eeas.europa.eu/delegations/council-europe/european-commission-signs-historic-council-europe-framework-convention-artificial-intelligence-and_en?s=51. Accessed 4 Dec. 2025.

B. National Frameworks

Brazil



■ AI in Brazil

<https://www.unesco.org/ethics-ai/en/brazil>

■ AI regulation in Brazil: Advancements, flows, and the need to learn from the data protection experience.

[https://www.sciencedirect.com/science/article/abs/pii/S0267364922001108#:~:text=Methodology.%20To%20develop%20this%20article%2C%20we%20conducted,Ministry%20of%20Science%2C%20Technology%2C%20and%20Innovation%20\(MCTI\).](https://www.sciencedirect.com/science/article/abs/pii/S0267364922001108#:~:text=Methodology.%20To%20develop%20this%20article%2C%20we%20conducted,Ministry%20of%20Science%2C%20Technology%2C%20and%20Innovation%20(MCTI).)

■ AI Governance in Brazil

<https://digital.nemko.com/regulations/ai-governance-brazil>

■ Updates on the Artificial Intelligence Bill (PL 2338/2023)

<https://www.leonardi.adv.br/en/insights/updates-on-the-artificial-intelligence-bill-pl-2338-2023/>

■ Brazil's path to responsible AI

<https://oecd.ai/en/wonk/brazils-path-to-responsible-ai>

■ Brazilian Legal Framework for AI

<https://irisbh.com.br/wp-content/uploads/2022/08/Brazilian-Legal-Framework-for-Artificial-Intelligence-Contributions-to-the-Federal-Senates-Jurists-Committee-IRIS.pdf>

Canada



- Treasury Board of Canada Secretariat (TBS)

https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/guide-scope-directive-automated-decision-making.html?utm_source=chatgpt.com

- OSFI — Guideline B-13: Technology & Cyber Risk Management (final 2022; effective 2024).

[osfi-bsif.gc.ca+1](https://osfi-bsif.gc.ca/1)

- OSFI — Guideline E-23: Model Risk Management (final Sept 11, 2025; effective May 1, 2027).

[osfi-bsif.gc.ca+2blakes.com+2](https://osfi-bsif.gc.ca/2blakes.com+2)

- Health Canada — Guidance Document: Software as a Medical Device (SaMD): Definition & Classification and Classification Examples.

[Government of Canada+2Government of Canada+2](#)

- Innovation, Science and Economic Development (ISED) — Canadian Artificial Intelligence Safety Institute (CAISI); Government announcement (Nov 12, 2024).

[ISED Canada+2Government of Canada+2](#)

- Government of Canada — Responsible use of AI in government (overview portal).

<https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai.html>

China



- Algorithmic Recommendation Provisions (effective Mar 1, 2022)

DigiChina+1

- Deep Synthesis Provisions (issued Dec 2022; in force Jan 2023)

chinalawtranslate.com+1

- Interim Measures for the Management of Generative AI Services (effective Aug 15, 2023) –

chinalawtranslate.com+2PwC+2

- AI Safety Governance Framework 1.0 (TC260, released Sept 9, 2024)

tc260.org.cn

- Measures for Labeling of AI-Generated Synthetic Content (issued Mar 2025; effective Sept 1, 2025)

chinalawtranslate.com+2insideprivacy.com+2

- Personal Information Protection Law (PIPL, effective Nov 1, 2021)

en.npc.gov.cn.cdurl.cn+1

- Data Security Law (DSL, 2021)

npc.gov.cn

- Cybersecurity Law (CSL, 2017)

DigiChina+1

- Context & analysis on algorithm regulation

<https://library.fes.de/pdf-files/bueros/bruessel/19904.pdf>

Finland



- EU AI Act — official: application timeline & obligations.

Digital Strategy

- AuroraAI (Finland MoF): human-centric, life-event-based public-service program; program background.

Valtioneuvosto+2Valtiovarainministerio+2

- FIN-FSA (DORA implementation): supervisory focus on ICT risk, incident reporting, and testing.

Financial Supervisory Authority

- Fimea (medical devices): competence & current 2025 market-surveillance campaign for software-based devices.

Fimea+1

- Valvira: national supervisory authority for welfare & health services.

Valvira+1

India



- DPDP Act 2023 (MeitY) – India’s data protection law

<https://www.meity.gov.in/content/digital-personal-data-protection-act-2023> (meity.gov.in)

- IndiaAI Mission – governance guidance (public consultation 2024/25)

<https://indiaai.gov.in/article/india-ai-governance-guidelines-empowering-ethical-and-responsible-ai> (IndiaAI)

- RBI – Draft Model Risk Management for AI/ML models (2024)

<https://www.fidcindia.org.in/wp-content/uploads/2024/08/RBI-DRAFT-MANAGEMENT-OF-MODEL-RISK-IN-CREDIT-05-08-24.pdf> (FIDC)

- RBI – Digital Lending Guidelines

<https://rbidocs.rbi.org.in/rdocs/notification/PDFs/GUIDELINESDIGITALENDINGD5C35A71D8124A0E92AEB940A7D25BB3.PDF> (rbidocs.rbi.org.in)

- RBI – IT / Outsourcing Directions (Master Direction on Outsourcing of IT Services)

https://www.rbi.org.in/scripts/BS_ViewMasDirections.aspx?id=12486 (rbi.org.in)

- DEPA / Account Aggregator framework (NBFC-AA Directions)

<https://sahamati.org.in/account-aggregator-master-direction-oct-5-2021/> (Sahamati)

- FIU-IND AML regime (FIU-IND official site)

<https://fiuindia.gov.in/> (fiuindia.gov.in)

- ABDM / NHA – national digital health rails (consent, registries, pilots)

<https://abdm.gov.in/> (Ayushman Bharat Digital Mission)

- CDSCO – Medical Devices Rules, 2017

<https://cdsco.gov.in/opencms/opencms/en/Acts-and-rules/Medical-Devices-Rules/> (cdsco.gov.in)

- SaMD alignment with IMDRF (core SaMD WG resource)

<https://www.imdrf.org/working-groups/software-medical-device-samd> (imdrf.org)

- BIS standards references for medical devices

<https://esic.gov.in/attachments/circularfile/bef02def366ab55bcf65110a9f194ffb.pdf> (esic.gov.in)

Japan



- AI Guidelines for Business (METI/MIC)

https://www.meti.go.jp/english/press/2024/0419_002.html

■ AI Strategy 2022 (Cabinet Office)

https://www8.cao.go.jp/cstp/ai/aistratagy2022en_ov.pdf

■ Human-Centric AI Principles (Cabinet Office)

<https://www8.cao.go.jp/cstp/english/humancentricai.pdf>

■ Act on the Protection of Personal Information (APPI) — English Translation

<https://www.japaneselawtranslation.go.jp/en/laws/view/4241>

■ Digital Society Priority Plan — Digital Agency

<https://www.digital.go.jp/en/policies/priority-policy-program>

■ Hiroshima AI Process — International Guiding Principles

<https://g7g20-documents.org/database/document/2023-g7-japan-leaders-leaders-annex-hiroshima-process-international-guiding-principles-for-organizations-developing-advanced-ai-system>

■ Hiroshima AI Process — Code of Conduct for Advanced AI Developers

<https://g7g20-documents.org/database/document/g7-hiroshima-process-code-of-conduct>

■ Society 5.0 — Government Concept Page

https://www8.cao.go.jp/cstp/society5_0/

■ Governance Guidelines for AI Principles Implementation

<https://www.meti.go.jp/press/2020/07/20200717002/20200717002.html>

■ METI AI Governance Documents Library

https://www.meti.go.jp/english/policy/mono_info_service/ai/

■ Digital Agency Homepage

<https://www.digital.go.jp/en>

■ OECD AI Principles (Japan signatory)

<https://oecd.ai/en/ai-principles>

■ APPI Amendment Explanatory Notes (2022)

<https://www.tmi.gr.jp/eyes/blog/2022/13236.html>

■ CSIS Report — Japan AI Governance Strategy

<https://www.csis.org/analysis/norms-new-technological-domains-japans-ai-governance-strategy>

Kenya



■ Consumer Protection Act – NO. 46 of 2012

<https://kecopac.go.ke/sites/default/files/publications/Consumer%20Protection%20Act%20No.%2046%20of%202012.pdf>

■ The Computer Misuse and Cybercrimes Act, 2018

<https://nc4.go.ke/the-computer-misuse-and-cybercrimes-act-2018/>

■ The Data Protection Act - NO. 24 of 2019

<https://www.kentrade.go.ke/wp-content/uploads/2022/09/Data-Protection-Act-1.pdf>

■ Kenya AI Strategy 2025 – 2030

<https://ict.go.ke/sites/default/files/2025-03/Kenya%20AI%20Strategy%202025%20-%202030.pdf>

■ Digital Economy Blueprint 2019

https://smartafrica.org/wp-content/uploads/2021/08/Kenya_Digital_Economy_2019.pdf

■ Draft Kenya Standard 3007:2024 - Information technology — Artificial Intelligence — Code of Practice for AI Applications

https://members.wto.org/crnattachments/2024/TBT/KEN/24_02705_00_e.pdf

■ National ICT Policy 2019

<https://ke-cirt.go.ke/wp-content/uploads/2021/07/NATIONAL-ICT-POLICY-2019.pdf>

■ Kenya Robotics and Artificial Intelligence Society Bill, 2023

https://www.dataguidance.com/sites/default/files/the_kenya_robotics_and_artificial_intelligence_society_bill_2023.docx.pdf

Saudi Arabia (KSA)



■ Saudi Data & AI Authority (SDAIA):

<https://sdaia.gov.sa/en>

■ Navigating AI Governance in Saudi Arabia: Regulations, Standards, and Global Alignment

<https://www.modulos.ai/blog/saudi-ai-regulations-guide/>

■ AI Regulation in KSA

<https://digital.nemko.com/regulations/ai-regulation-in-saudi-arabia>

■ AI Ethics Principles:

<https://sdaia.gov.sa/en/SDAIA/about/Files/AIAdoptionFramework.pdf>

■ Gen AI Guidelines for Government

<https://sdaia.gov.sa/en/SDAIA/about/Files/GenAIGuidelinesForGovernmentENCompressed.pdf>

■ AI Law in KSA

<https://www.lw.com/admin/upload/SiteAttachments/Lexology-In-Depth-Artificial-Intelligence-Law-Saudi-Arabia.pdf>

■ Navigating AI Governance in Saudi Arabia: Regulations, Standards, and Global Alignment

<https://www.modulos.ai/blog/saudi-ai-regulations-guide/>

Singapore



■ Artificial Intelligence in Singapore

<https://www.imda.gov.sg/about-imda/emerging-technologies-and-research/artificial-intelligence>

■ Governing intelligence: Singapore

https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=6527&context=sol_research

■ Singapore's Approach to AI Governance

<https://www.pdpc.gov.sg/help-and-resources/2020/01/model-ai-governance-framework>

■ AI Governance Framework – Second Edition

<https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf>

■ AI Verify

<https://fpf.org/blog/ai-verify-singapores-ai-governance-testing-initiative-explained/>

- Personal Data Protection Commission (PDPC) - Model AI Governance Framework (2nd Edition):

<https://www.pdpc.gov.sg/>

- AI Verify Foundation - Model AI Governance Framework for Generative AI (GenAI Framework):

<https://aiverifyfoundation.sg/>

- AI Verify Foundation - What is AI Verify?:

<https://aiverifyfoundation.sg/>

- Infocomm Media Development Authority (IMDA) - Artificial Intelligence overview:

<https://www.imda.gov.sg/>

- Personal Data Protection Commission (PDPC) - Home/General Resources:

www.pdpc.gov.sg

- Monetary Authority of Singapore (MAS) - Artificial Intelligence Model Risk Management (FEAT Principles/Veritas Framework context):

<https://www.mas.gov.sg/>

South Africa



- Protection of Personal Information Act, 2013

https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf

- Consumer Protection Act, 2008

https://www.gov.za/sites/default/files/32186_467.pdf

■ Cybercrimes Act, 2020

https://www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf

■ National AI Government Summit Discussion Document

https://www.dcdt.gov.za/images/phocadownload/AI_Government_Summit/National_AI_Government_Summit_Discussion_Document.pdf

■ Report of the Presidential Commission on the Fourth Industrial Revolution

https://www.gov.za/sites/default/files/gcis_document/202010/43834gen591.pdf

■ South Africa National AI Policy Framework

<https://www.dcdt.gov.za/sa-national-ai-policy-framework/file/338-sa-national-ai-policy-framework.html>

South Korea



■ Basic Act on the Development of Artificial Intelligence and Establishment of Foundation for Trustworthiness (AI Basic Act)

<https://aibasicact.kr/> (aibasicact.kr)

■ Overview: South Korea Artificial Intelligence (AI) Basic Act — summary article (Trade.gov)

<https://www.trade.gov/market-intelligence/south-korea-artificial-intelligence-ai-basic-act> (Trade.gov)

■ National Guidelines for AI Ethics (2020) / “AI for Humanity” ethics standards — as referenced in OECD Review

https://www.oecd.org/en/publications/digital-government-review-of-korea_9defc197-en/full-report/leveraging-ai-for-government-transformation_64eb9a1e.html (see Box 5.3) (OECD)

- Amendment to the Personal Information Protection Act (PIPA) — automated decision-making & data protection provisions

https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/10/artificial-intelligence-and-the-labour-market-in-korea_af668423/68ab1a5a-en.pdf (OECD)

- Analysis: “Framework Act on the Development of Artificial Intelligence and Establishment of Trust” (English translation & overview) — CSET / Georgetown

<https://cset.georgetown.edu/publication/south-korea-ai-law-2025/> (CSET)

- Practice Guide: Artificial Intelligence 2025 — South Korea (Chambers & Partners)

<https://practiceguides.chambers.com/practice-guides/artificial-intelligence-2025/south-korea> (Global Practice Guides)

- Analysis / Commentary: “AI Security Strategy and South Korea’s Challenges” (CSIS)

<https://www.csis.org/analysis/ai-security-strategy-and-south-koreas-challenges> (CSIS)

- Summary of South Korea AI policies and regulations (JustAI)

<https://justai.in/ai-policies-and-regulations-in-korea/> (JustAI)

United Arab Emirates (UAE)



- The Official Platform of the UAE Government (u.ae):

UAE Strategy for Artificial Intelligence

- UAE Legislation Portal

<https://uaelegislation.gov.ae/>

- The UAE Charter for the Development and Use of AI

<https://uaelegislation.gov.ae/en/policy/details/the-uae-charter-for-the-development-and-use-of-artificial-intelligence>

- UAE’s International Stance on Artificial Intelligence Policy

<https://uaelegislation.gov.ae/en/policy/details/uae-s-international-stance-on-artificial-intelligence-policy>

United Kingdom (UK)



- A pro-innovation approach to AI regulation (White Paper):

www.gov.uk

- Launching the Artificial Intelligence Playbook (GDS blog):

<https://gds.blog.gov.uk/2025/02/10/launching-the-artificial-intelligence-playbook-for-the-uk-government/>

- AI Security Institute (AISI) Official Website:

<https://www.aisi.gov.uk/>

- Establishing a pro-innovation approach to regulating AI (Policy Paper PDF):

https://assets.publishing.service.gov.uk/media/62d7feaae90e071e772445cd/_CP_728_-_Establishing_a_pro-innovation_approach_to_regulating_AI.pdf

- ICO's strategic approach to regulating AI

<https://www.rpclegal.com/snapshots/data-protection/summer-2024/the-icos-strategic-approach-to-regulating-ai/>

- FCA's AI update (PDF report):

<https://www.fca.org.uk/publication/corporate/ai-update.pdf>

- UK AI Regulation: Current Status and Outlook (GDPR Local article):

<https://gdprlocal.com/uk-ai-act/>

- The UK's framework for AI regulation (Deloitte analysis):

<https://www.deloitte.com/uk/en/blogs/ecrs/the-uks-framework-for-ai-regulation.html>

- 9 Key AI Governance Frameworks in 2025 (AI21 Labs analysis):

<https://www.ai21.com/knowledge/ai-governance-frameworks/>

- Artificial Intelligence Playbook for the UK Government published (Burges Salmon article):

<https://www.burges-salmon.com/articles/102jzoi/artificial-intelligence-playbook-for-the-uk-government-published/>

United States (US)



- A centralized hub for U.S. government AI strategy and action plans

AI.gov Portal

- The White House (OSTP and Presidential Actions):

America's AI Action Plan (Official PDF)
E.O. 14179 "Removing Barriers..." (Official Source)
White House Office of Science and Technology Policy (OSTP)

- National Institute of Standards and Technology (NIST):

NIST AI Risk Management Framework (AI RMF) Homepage
NIST AI RMF 1.0 Publication (PDF)

- General Services Administration (GSA)

GSA AI Guidance and Resources
AI Guide for Government

6.2 Appendices

Appendix A: Glossary of Key Terms

This glossary compiles key terms and definitions used throughout the “Global AI Governance Frameworks: Comparative Study” document

Term	Definition
Accountability	The obligation of an organization or individual is to account for their activities, accept responsibility for them, and transparently disclose the results.
Algorithmic Bias	Systematic and repeatable errors in a computer system that create unfair outcomes, such as privileging one arbitrary group of users over others.
Artificial Intelligence (AI)	A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.
Binding Regulation	A rule or directive made and maintained by a legally enforceable authority.
Explainability	The extent to which the internal mechanics of a machine learning system can be explained in human terms.
Fairness	The quality of making judgments that are free from discrimination. In AI, this relates to ensuring that algorithmic decisions do not create or perpetuate unfair biases.
Governance Framework	A set of rules, principles, standards, and processes that guide the development, deployment, and use of AI.
Horizontal Regulation	A regulation that applies broadly across many different sectors and industries.
Human-in-the-Loop	A model that requires human interaction to assist the AI system in making decisions, especially in ambiguous cases.
Interoperability	The ability of different information systems, devices, and applications to access, exchange, integrate, and cooperatively use data in a coordinated manner.
Risk-Based Approach	A regulatory approach that tailors the level of scrutiny and intervention to the level of risk posed by an AI system.
Soft Law	Non-binding rules, principles, and guidelines that are not legally enforceable but can shape behavior and norms.
Transparency	The quality of being easy to perceive or understand. In AI, this refers to providing information about how an AI system operates and the data it utilizes.
Vertical Regulation	A regulation that applies to a specific industry or sector.

Appendix B: Abbreviations and Acronyms

Acronym	Full Form
AI	Artificial Intelligence
AICTO	Arab Information and Communication Technologies Organization
AIDA	Artificial Intelligence and Data Act (Canada)
AIGO	AI Governance Working Group (OECD)
AISI	AI Safety Institute (UK)
ALKS	Automated Lane Keeping Systems
ASEAN	Association of Southeast Asian Nations
AU	African Union
BRICS	Brazil, Russia, India, China, South Africa
CA	Canada
CAC	Cyberspace Administration of China
CoE	Council of Europe
DADM	Directive on Automated Decision-Making (Canada)
DIFC	Dubai International Financial Centre (UAE)
DPDP	Digital Personal Data Protection
DSIT	Department for Science, Innovation and Technology (UK)
ECOA	Equal Credit Opportunity Act (US)
EEOC	Equal Employment Opportunity Commission (US)
EHDS	European Health Data Space
EU	European Union
FDA	Food and Drug Administration (US)
FDA	Food and Drug Administration (US)
FEAT	Fairness, Ethics, Accountability, and Transparency (Singapore)
Fintech	Financial Technology
FTC	Federal Trade Commission (US)
G20	Group of Twenty
G7	Group of Seven
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation (EU)
GPAI	Global Partnership on AI

HR	Human Resources
HUDERIA	Human Dignity, Human Rights, Democracy, Equality, Rule of Law, and Individual Autonomy
IAWG-AI	Inter-Agency Working Group on AI (UN)
ICESCO	Islamic World Educational, Scientific and Cultural Organization
ICO	Information Commissioner's Office (UK)
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IMDA	Infocomm Media Development Authority (Singapore)
INAIL	International Network of AI Integrity Institutes
ISED	Innovation, Science and Economic Development (Canada)
ISO	International Organization for Standardization
ITU	International Telecommunication Union
KSA	Kingdom of Saudi Arabia
LAC	Latin America and the Caribbean
MAS	Monetary Authority of Singapore
MHRA	Medicines and Healthcare products Regulatory Agency (UK)
MIIT	Ministry of Industry and Information Technology (China)
NIST	National Institute of Standards and Technology (US)
NIST	National Institute of Standards and Technology (US)
OECD	Organization for Economic Co-operation and Development
ONE AI	OECD Expert Network on AI
PCCP	Predetermined Change Control Plan
PDPC	Personal Data Protection Commission (Singapore)
RMF	Risk Management Framework
SDAIA	Saudi Data & AI Authority
TBS	Treasury Board of Canada Secretariat
UAE	United Arab Emirates
UN	United Nations
UNECE	United Nations Economic Commission for Europe
UNESCO	United Nations Educational, Scientific and Cultural Organization
WEF	World Economic Forum

Appendix C: Glossary of Consolidated Comparative Matrix – National Level

1. A **domain** is the set of entities to which the governance framework applies.

- **Public Sector:** The rules apply strictly to government agencies and public administration bodies.
- **Private Sector:** The rules apply strictly to commercial businesses and non-governmental organizations.
- **Both:** A unified framework where the same core principles or laws apply universally to all entities, whether government or private.
- **Split (Public/Private):** A dual system where strict mandatory rules regulate the government, while the private sector operates under a separate, voluntary regime.

2. **Scope** refers to the depth and focus of the regulation.

- **High-level Policy Principles:** Broad ethical values (e.g., “AI must be fair”) without technical specifications on how to achieve them.
- **Technical / Operational Standards:** Detailed engineering specifications, “how-to” benchmarks, or specific performance metrics (e.g., NIST RMF).
- **Principles Applied Vertically:** High-level ethical principles are interpreted and enforced separately by each industry regulator (e.g., a Bank regulator vs. a Health regulator) rather than by a central AI authority.
- **Technical (Filings):** A bureaucratic scope focusing on the mandatory registration of algorithms and security reviews with the state (specific to China).
- **Principles + “Techno-legal”:** Governance that combines legal rules with digital public infrastructure where compliance is “hard-coded” into the software platforms (specific to India).
- **Legal / Rights-based:** A scope focused primarily on protecting fundamental human rights (privacy, non-discrimination) through binding statutes, allowing citizens to challenge AI decisions legally.
- **Operational Governance:** Focuses on the internal management structure of a company (e.g., establishing ethics committees, accountability logs) rather than the technology itself.

3. **Legal Nature** refers to the binding force of the governance.

- **Mandatory (Binding):** Codified in a statute or act; compliance is non-negotiable, and violations result in penalties.
- **Mandatory (Proposed):** A binding law is currently in the legislative process; it creates “pre-compliance” pressure but is not yet enforceable.
- **Voluntary:** Compliance is optional; organizations adopt the framework for ethical reasons or internal quality control with no legal penalty for non-compliance.
- **Voluntary (Soft Law):** Technically non-binding but carries “quasi-legal” weight because regulators expect adoption; non-compliance is viewed as negligence or invites scrutiny.

- **Hybrid (Data Law + Voluntary):** A dual-track system where AI design is voluntary, but the data used to train it is strictly regulated by binding Personal Data Protection Laws.
- **Hybrid (Laws + Advisory):** Core AI rules are advisory (suggestions), but the government uses other “hard” laws (like Cybercrimes or IT Acts) to enforce compliance indirectly.

4. **Regulatory Approach** Refers to the government’s strategy for managing the sector.

- **Statutory / Binding:** Rules are set by parliament/congress as formal laws.
- **Voluntary Guidance / Standards:** The government issues “best practices” to guide the industry without the force of law.
- **Sector-led / Non-prescriptive:** Existing industry regulators (e.g., Finance, Energy) create specific rules for their domains; the government avoids a “one-size-fits-all” law.
- **Agile / Innovation-first:** The regulatory focus is on speed and adaptability; rules are kept minimal to encourage rapid technological development.
- **Soft Regulation + Sandboxes:** The government allows companies to test innovative AI in a controlled environment (“sandbox”) with relaxed rules to observe impacts before regulating.

5. **Methodology** refers to the philosophical basis of the rules.

- **Risk-Based:** The strictness of the regulation scales with the potential harm (e.g., a chatbot has fewer rules than a medical diagnosis AI).
- **Principles-Based:** The regulation defines the desired outcome (e.g., “Must be safe”) but leaves the method of achieving it up to the organization.
- **Risk-Based (Security & Control):** A variation of risk-based methodology heavily focused on national security, content control, and social stability (specific to China).

6. **Risk Management Methodology** refers to the specific mechanism used to handle risk.

- **Risk-Tiered Approach:** A rigid classification system where AI systems are labeled (e.g., “Unacceptable,” “High,” “Limited”) and legal obligations are assigned based on the label.
- **Process-Based Guidance:** Requires organizations to follow a continuous process (e.g., Map, Measure, Manage) throughout the AI lifecycle, rather than fitting into a static tier.
- **Process-Based (Internal Gov):** Focuses on establishing internal corporate accountability structures (committees, officers) to manage risk.
- **Process-Based (Lifecycle):** Controls are applied at every stage of development, from data collection to model deployment and monitoring.

7. Enforcement & Compliance Mechanisms refers to how the rules are policed.

- **Formal Certification & Auditing:** Third-party verification is required; companies must prove safety before deploying high-risk systems.
- **Administrative Filings:** Companies must submit technical documentation to the government for review and registration.
- **Documentation and Reporting:** Companies must maintain internal logs of their AI's performance and decision-making for potential review.
- **Centralized Oversight:** A single, dedicated government body (e.g., AI Commission) is responsible for policing all AI activities.
- **Existing Regulators:** Enforcement is decentralized; a bank uses banking laws to punish AI errors, while a hospital uses health laws.
- **Market-driven / Reputational:** There is no direct government enforcer; compliance is driven by the fear of losing customers or brand damage.
- **Management Oversight:** In public sector contexts, senior government officials are personally responsible for ensuring their departments comply.

Appendix D: Glossary of Consolidated Comparative Matrix – Sectoral Level

1. Model: Refers to the classification archetype assigned to the sector based on its governance maturity and risk profile.

- **High-Stakes / Hard Law:** Sectors where failure poses immediate threats to life, safety, or financial stability, triggering binding government enforcement.
- **Industrial / Standardized:** Sectors where governance is driven by technical reliability and supply chain interoperability rather than political regulation.
- **Emerging / Strategic:** Sectors where governance is currently “soft” or strategic to encourage adoption, though specific high-risk use cases may be regulated.

2. Regulatory Focus Refers to the primary “target” or focus of the regulation in that sector.

- **Safety & Ethics:** Focuses on patient safety, physical integrity, and bio-ethical principles (e.g., autonomy). Source: WHO Ethics & Governance of AI for Health
- **Safety & Liability:** Focuses on the physical operation of vehicles and the legal attribution of fault (who is responsible?) in accidents. Source: UNECE Regulation No. 157
- **fairness / Explainability:** Focuses on preventing algorithmic discrimination and ensuring decisions, such as loan denials, can be clearly explained. Source: CFPB Joint Statement on Credit Underwriting
- **Quality & Safety:** Focuses on product consistency and preventing defects in physical machinery and robotics. Source: ISO/IEC 42001 Scope
- **Security & Efficiency:** Focuses on protecting critical infrastructure from cyberattacks and managing energy resource consumption. Source: ISO/IEC 27001 Overview

- **Rights & Literacy:** Focuses on protecting fundamental human rights and building workforce skills. *Source:* UNESCO Guidance for Policy-Makers
- **Supply Chain / Labor:** Focuses on the ethical sourcing of data/materials and the management of agricultural workforces. *Source:* OECD-FAO Guidance for Responsible Supply Chains

3. Legal Nature refers to the binding force of the governance framework.

- **Mandatory (Binding):** Codified in a specific statute or administrative rule; compliance is non-negotiable. *Source:* EU AI Act High-Risk Classification
- **Mandatory (Existing Law):** The sector is governed by pre-AI laws (e.g., ECOA) that are legally interpreted to apply strictly to AI models. *Source:* CFPB Circular on Adverse Action
- **Voluntary (Standards):** Compliance is technically optional but effectively mandatory for market access due to supply chain requirements. *Source:* ISO/IEC 42001 Certification
- **Hybrid (Standards + Law):** A mix where security is governed by technical standards (ISO 27001), but specific aspects (like energy reporting) are governed by binding law. *Source:* IEA AI Guidelines
- **Voluntary (Soft Law):** Guidelines or principles that encourage best practices but carry no direct legal penalty for non-compliance. *Source:* OECD Principles on Artificial Intelligence

4. Regulatory Approach: Refers to the mechanism used by the authority to manage the sector.

- **Statutory / Lifecycle:** The regulator enforces rules throughout the product's entire life, from design to post-market updates. *Source:* FDA AI/ML Action Plan
- **International Regs:** Governance is set by a global treaty-level body to ensure cross-border harmonization. *Source:* UNECE WP.29
- **Interagency Guidance:** Multiple regulators (e.g., Fed, CFPB) issue joint statements to clarify how existing laws apply to AI. *Source:* US Treasury AI Report
- **Policy Guidance:** High-level recommendations intended to shape government policy and curriculum rather than direct technical rules. *Source:* MahaAgri-AI Policy 2025–2029 (India)
- **Strategic Roadmaps:** The government issues a long-term plan to promote adoption and build capacity rather than policing immediate use. *Source:* MahaAgri-AI Policy 2025–2029
- **Industry-Led:** The private sector develops consensus standards (e.g., ISO/IEEE) which become the de facto rules for the industry, rather than government mandates. *Source:* ISO/IEC 42001 Overview (ANAB)

- **Sector-Specific:** Rules are explicitly tailored to the unique operational risks of that industry (e.g., grid stability, pipeline pressure) rather than generic AI rules. Source: IEA Guidelines for the Energy Sector

5. Risk Management Method refers to the specific methodology used to manage risk

- **Risk-Tiered (EU/FDA):** A rigid classification system where AI uses are labeled (e.g., “High-Risk”), and obligations are assigned based on the label. Source: EU AI Act (Risk Classification)
- **Process-Based (Adverse Action):** Compliance is achieved by following a specific legal process (e.g., providing a reason for denial) rather than passing a technical test. Source: Singapore FEAT Principles
- **Process-Based (ISO 42001):** Focuses on establishing an internal management system to identify and mitigate risks continuously. Source: ISO/IEC 42001:2023 Standard
- **Principles-Based (Human-Centric / Sustainability):** Focuses on aligning AI with broad human values and environmental goals. Source: UNESCO Guidance for Policy-Makers
- **Risk-Tiered / Black Box:** Includes specific requirements to record operational data (DSSAD) to determine liability after an incident. Source: UN Regulation No. 157 - Automated Lane Keeping Systems
- **Risk-Based (Cybersecurity):** Focuses specifically on hardening systems against external attacks and ensuring resilience. Source: ISO/IEC 27001: Information security, cybersecurity, and privacy protection
- **Enforcement:** Refers to how the rules are policed.
- **Pre-Market Approval:** The regulator must review and license the AI system *before* it can be sold or deployed. Source: FDA Premarket Submissions Guidance
- **Type Approval / Homologation:** A vehicle or component must be certified as meeting technical specifications before mass production can begin. Source: UNECE Regulation No. 157
- **Third-Party Certification:** An independent auditor verifies compliance with a standard to validate the company’s claims. Source: ISO/IEC 42001 Certification
- **Soft / EU High-Risk Exceptions:** Unenforceable guidance, except for specific use cases (like grading/labor) that trigger binding EU AI Act enforcement. Source: EU AI Act High-Risk List
- **Existing Agencies:** Enforcement is carried out by traditional bodies (e.g., Consumer Protection Bureaus) using their standard powers. Source: Joint Statement on Machine Learning in Credit Underwriting
- **Critical Infra Protection:** Enforcement is driven by national security mandates to protect essential services (power/water). Source: EU AI Act (Critical Infrastructure Classification) and US DOE AI Usage Guidelines



1. Brazil

- **Issuing Organization and Mandate:** The Temporary Commission on Artificial Intelligence (CTIA) and the Brazilian government. The mandate is to establish a national legal framework for AI that balances innovation with human rights and democratic values.
- **Legal and Regulatory Approach:** A proposed AI Bill (PL 2020/21) that is a binding, risk-based legislative framework.
- **Core Principles and Objectives:** The bill explicitly lists core principles such as respect for human rights, non-discrimination, transparency, human oversight, and the protection of personal data.
- **Scope and Applicability:** The proposed bill covers the entire lifecycle of AI systems, from conception to governance, with specific regulations for «high-risk» systems.
- **Governance Structure:** The proposed bill suggests a governance structure that includes a central authority and a focus on sectoral action to ensure compliance with existing laws like the General Data Protection Law (LGPD).
- **Enforcement Mechanisms:** The proposed bill includes strict liability for damages caused by AI and financial penalties of up to R50\$ million or %2 of a company's turnover.
- **Strengths and Weaknesses:** The framework provides clear guidance and legal certainty with a strong focus on human rights. A weakness is that it is still a proposed law, and its future is not yet certain.
- **International Alignment:** Brazil's proposed bill has clear parallels with the EU AI Act, demonstrating the global influence of the EU framework.



2. Canada

- **Issuing Organization and Mandate:** The government of Canada, through the proposed Artificial Intelligence and Data Act (AIDA). The mandate is to establish a foundational framework for the responsible design, development, and deployment of AI systems that impact the lives of Canadians.
- **Legal and Regulatory Approach:** A proposed binding, risk-based legislative approach that has not yet passed into law. It is complemented by a voluntary Code of Conduct for generative AI.
- **Core Principles and Objectives:** To ensure that AI systems deployed in Canada are safe and non-discriminatory, while also supporting responsible innovation. It focuses on identifying, assessing, and mitigating risks of harm and bias, particularly in «high impact» systems.
- **Scope and Applicability:** The proposed AIDA would apply to businesses involved in high-impact AI systems.
- **Governance Structure:** The proposed framework would establish an AI and Data Commissioner to oversee compliance, conduct third-party audits, and enforce the act.

- **Enforcement Mechanisms:** AIDA outlines administrative monetary penalties and prosecution for criminal offenses. The Minister of Innovation, Science, and Industry would have the power to order an audit or even shut down a system in cases of imminent harm.
- **Strengths and Weaknesses:** The framework is designed to be flexible and interoperable with other international standards. Its main weakness is that it is still a proposed law, and its final form and implementation are not yet certain.
- **International Alignment:** The framework is designed to be interoperable with existing and future regulatory approaches and aligns with international discussions on AI regulation.

3. China



- **Issuing Organization and Mandate:** Primarily the Cyberspace Administration of China (CAC), along with other bodies like the Ministry of Science and Technology (MOST). The mandate is to control the development and use of AI to ensure national security, public welfare, and data privacy.
- **Legal and Regulatory Approach:** A multi-level, mandatory, and risk-based framework. It is composed of a series of targeted regulations for specific technologies (e.g., algorithmic recommendation, deep synthesis) and a planned future comprehensive AI law.
- **Core Principles and Objectives:** To ensure that AI serves the CCP's agenda, promoting political and social stability. It mandates that AI systems respect public order, morality, and socialist values.
- **Scope and Applicability:** The regulations are technology-specific and apply to all AI services with «public opinion attributes or social mobilization capabilities.»
- **Governance Structure:** A highly centralized and top-down governance model where the CAC is the main regulator and enforces compliance through security assessments and filings.
- **Enforcement Mechanisms:** Compliance is enforced through security assessments and algorithm filings with the CAC. Non-compliance can lead to severe penalties, including service suspension and criminal liability.
- **Strengths and Weaknesses:** The framework's strength is its clear, enforceable rules and its ability to rapidly implement new regulations. A major weakness is the potential for stifling innovation and the prioritization of state control over individual freedoms.
- **International Alignment:** China aims to offer a «Chinese model» for global AI governance, balancing efficiency, and safety, while also participating in international forums.

4. Finland



- **Issuing Organization and Mandate:** As an EU member state, Finland's AI framework is governed by the EU AI Act. The mandate is to ensure AI systems are safe, respect fundamental rights, and foster innovation within a single European market.
- **Legal and Regulatory Approach:** The EU AI Act is a binding, risk-based legislative framework. Finland is now working to propose supplementary national legislation to support its implementation.
- **Core Principles and Objectives:** The framework aims to protect fundamental rights and safety, encourage investment and innovation, and create a single, unified market for lawful and trustworthy AI.
- **Scope and Applicability:** The Act applies to all organizations that develop, deploy, import, or distribute AI models or systems to the EU. It is extraterritorial, meaning it also applies to non-EU companies whose AI outputs are used in the EU.
- **Governance Structure:** A centralized governance model at the EU level with national competent authorities in each member state responsible for enforcement.
- **Enforcement Mechanisms:** Non-compliance can result in significant financial penalties, with fines of up to 35€ million or %7 of worldwide annual turnover for breaches of prohibited AI system requirements.
- **Strengths and Weaknesses:** Its main strength is a high degree of legal certainty and a comprehensive, clear set of rules. A potential weakness is that its prescriptive nature may be slow to adapt to new technological advancements.
- **International Alignment:** It is a pioneering global framework that is influencing AI legislation in other countries, such as Brazil and Canada.

5. India



- **Issuing Organization and Mandate:** The National Cyber and AI Center (NCAIC) as part of the India AI Mission. The mandate is to create a national framework that promotes human-centric and inclusive AI development.
- **Legal and Regulatory Approach:** India is in the process of formulating a risk-based framework, but currently lacks a central, binding law. It relies on existing laws like the Digital Personal Data Protection Act.
- **Core Principles and Objectives:** To ensure AI is used for inclusive growth and to address challenges like fragmented governance and a lack of ethical frameworks.
- **Scope and Applicability:** The draft «AI Governance Framework for India 26-2025» is intended to be applicable across all sectors.
- **Governance Structure:** India's governance is currently fragmented, with multiple agencies overseeing distinct aspects of AI. The draft framework aims to create a more unified, whole-of-government approach.
- **Enforcement Mechanisms:** Enforcement is currently limited and relies on existing data protection and consumer protection laws. There is a need for a clear, constitutional AI law to hold entities accountable for failures.

- **Strengths and Weaknesses:** The framework's objective of using AI to benefit a diverse, large population is a strength. A key weakness is the lack of a central, legally binding framework, which can lead to ambiguity and a lack of public trust.
- **International Alignment:** The framework is influenced by global trends but aims to build a model that is appropriate for India's unique challenges and priorities.

6. Japan



- **Issuing Organization and Mandate:** The Japanese government, with the Prime Minister leading the AI Strategic Headquarters. The mandate is to promote AI development and innovation while mitigating risk.
- **Legal and Regulatory Approach:** A «soft law» approach consisting of the non-binding AI Promotion Act, which is a strategic framework. It is supplemented by guidelines and clarifications on existing laws (e.g., copyright and data privacy).
- **Core Principles and Objectives:** To become the «world's most AI-friendly country.» The framework rests on four principles: enhancing international competitiveness, promoting AI comprehensively, ensuring transparency, and leading international cooperation.
- **Scope and Applicability:** The framework is applicable across all sectors, but its implementation relies on voluntary cooperation from businesses, academia, and citizens.
- **Governance Structure:** A multi-stakeholder governance model with the government providing a strategic plan, and businesses and academia encouraged to align voluntarily.
- **Enforcement Mechanisms:** There are no specific penalties or sanctions under the AI Promotion Act. Enforcement for inappropriate use is managed under existing legal frameworks, such as copyright and data privacy laws.
- **Strengths and Weaknesses:** Its strength is its flexibility and ability to adapt to technological change without being a deterrent to innovation. The main weakness is the lack of a binding, enforceable framework, which can lead to compliance ambiguities.
- **International Alignment:** Japan actively contributes to international norms and guidelines, and its framework is more complementary than contradictory to the EU's risk-based approach.

7. Kenya



- **Issuing Organization and Mandate:** The Kenyan government has a National AI Strategy 2030–2025. The mandate is to position Kenya as a leader in AI adoption and governance in Africa, fostering socio-economic development.

- **Legal and Regulatory Approach:** The country lacks a dedicated AI legal framework, relying on existing laws like the Data Protection Act and a developing AI Code of Practice. The strategy is to implement a «soft» regulatory framework that balances innovation and safeguards.
- **Core Principles and Objectives:** The strategy's key goals include fostering ethical AI, enhancing public service delivery, and bridging the digital divide to ensure AI benefits marginalized communities.
- **Scope and Applicability:** The framework targets key sectors for AI integration, including healthcare, agriculture, and finance.
- **Governance Structure:** The governance structure is still in development, with the strategy advocating for inter-agency coordination and public-private partnerships.
- **Enforcement Mechanisms:** Currently, enforcement is based on existing data protection and cybercrime laws. The government plans to use «regulatory sandboxes» to refine future governance and compliance standards.
- **Strengths and Weaknesses:** The strategy is forward-looking and focuses on practical applications to address national challenges. A key weakness is the absence of a comprehensive legal framework and a detailed implementation roadmap, which creates regulatory uncertainty.
- **International Alignment:** The strategy aims to align with regional and global AI governance trends.

8. Saudi Arabia



- **Issuing Organization and Mandate:** The Saudi Data and Artificial Intelligence Authority (SDAIA). The mandate is to position Saudi Arabia as a global AI leader by 2030 through its National Strategy for Data and Artificial Intelligence (NSDAI).
- **Legal and Regulatory Approach:** The framework is currently based on a national strategy, supplemented by ethical principles and a proposed «Draft Global AI Hub Law.»
- **Core Principles and Objectives:** The NSDAI aims to accelerate innovation, attract investment and talent, and ensure the ethical use of AI in line with the country's values.
- **Scope and Applicability:** The national strategy is broad and applies across all sectors.
- **Governance Structure:** A centralized governance structure where the SDAIA guides AI policy and development.
- **Enforcement Mechanisms:** Enforcement is currently based on the principles published by SDAIA, with a formal enforcement mechanism to be established in future legislation.
- **Strengths and Weaknesses:** A strength is the ambitious, high-level strategy backed by a national authority. A weakness is the lack of a legally binding, detailed framework, which may create uncertainty for businesses.
- **International Alignment:** The framework aims to be globally competitive and aligned with international best practices.



9. Singapore

- **Issuing Organization and Mandate:** The Infocomm Media Development Authority (IMDA) and the AI Verify Foundation. Their mandate is to provide a practical guide for organizations to address key ethical and governance issues in a «trust-by-design» approach.
- **Legal and Regulatory Approach:** A «soft law» approach, meaning the framework is voluntary and non-binding. It is meant to be a guide rather than a strict set of rules.
- **Core Principles and Objectives:** To build a trusted AI ecosystem by focusing on nine dimensions of trust, such as accountability, fairness, and transparency.
- **Scope and Applicability:** The framework is applicable to all private sector organizations, with a specific focus on generative AI models and solutions.
- **Governance Structure:** The framework encourages a multi-stakeholder and consensual approach, with key input from government and industry.
- **Enforcement Mechanisms:** Compliance is voluntary, relying on market mechanisms and industry best practices.
- **Strengths and Weaknesses:** The framework is highly adaptable and innovation friendly. However, its non-binding nature may be a weakness in ensuring consistent and mandatory safeguards.
- **International Alignment:** The framework has influenced regional initiatives, such as the ASEAN Guide on AI Governance and Ethics. Singapore actively collaborates with international partners like the World Economic Forum.



10. South Africa

- **Issuing Organization and Mandate:** The Department of Communications and Digital Technologies (DCDT). The mandate is to promote the integration of AI to drive economic growth and societal well-being.
- **Legal and Regulatory Approach:** The National AI Policy Framework is a foundational, non-binding document and a first step towards creating a comprehensive national AI policy. It is currently supported by existing data protection laws like the Protection of Personal Information Act (POPIA).
- **Core Principles and Objectives:** The framework emphasizes ethical AI development, talent development, digital infrastructure, and data privacy to ensure AI benefits are widely shared and risks are managed effectively.
- **Scope and Applicability:** The framework is intended to apply across all sectors of society.
- **Governance Structure:** The framework seeks to promote a coordinated approach among government, academia, and the private sector.
- **Enforcement Mechanisms:** Enforcement is currently subject to existing laws like POPIA. There are no new enforcement mechanisms or penalties specifically for AI.
- **Strengths and Weaknesses:** It provides a clear foundational vision for ethical and inclusive AI development. A major weakness is that it is not yet a dedicated law, which can lead to a lack of legal clarity.

- **International Alignment:** The framework aligns with the African Union's AI strategy and aims to position South Africa as a leader in global AI ethics and governance discussions.

11. South Korea



- **Issuing Organization and Mandate:** The South Korean government, with the Ministry of Science and ICT (MSIT) leading development. The mandate is to balance innovation with ethical AI development to position the country as a global AI powerhouse.
- **Legal and Regulatory Approach:** A binding, risk-based legal framework through the comprehensive AI Basic Act, which was signed into law in January 2025 and will take effect in January 2026.
- **Core Principles and Objectives:** The Act is guided by principles of transparency, human oversight, safety, and non-discrimination. Its main objective is to establish a unified, trustworthy foundation for AI.
- **Scope and Applicability:** The law applies to all AI activities that impact the South Korean market, including high-impact AI systems and generative AI, and it has an extraterritorial reach.
- **Governance Structure:** The framework is centered on a National AI Committee, which coordinates national initiatives, and the MSIT oversees compliance.
- **Enforcement Mechanisms:** The Act introduces fines and potential imprisonment for violations. It also requires impact assessments for high-impact AI systems.
- **Strengths and Weaknesses:** A strength is that it provides a clear, unified legal framework that balances innovation and regulation. A weakness is that it does not currently ban any AI systems outright, unlike the EU AI Act.
- **International Alignment:** South Korea's framework shares features with the EU AI Act and is designed to align with global standards.

12. United Arab Emirates



- **Issuing Organization and Mandate:** The UAE government, specifically the Artificial Intelligence and Advanced Technology Council (AIATC). The mandate is to make the UAE a world leader in AI and create a safe and ethical AI ecosystem.
- **Legal and Regulatory Approach:** A multi-layered approach consisting of a national strategy and non-binding guidelines for both the public and private sectors. It is also supported by existing data protection laws.

- **Core Principles and Objectives:** To accelerate AI adoption across government services and the economy. The AI Ethics Guide emphasizes principles like fairness, transparency, and human oversight.
- **Scope and Applicability:** The framework has a broad national scope, with specific regulations in financial free zones like the DIFC and ADGM.
- **Governance Structure:** A centralized structure led by the AIATC, with federal initiatives and specific frameworks for different zones and ministries.
- **Enforcement Mechanisms:** Enforcement relies on existing data protection laws and specific regulations in free zones. The frameworks are primarily non-binding, focusing on guidelines rather than penalties.
- **Strengths and Weaknesses:** A strength is the government's strong commitment and clear strategy, which is well-resourced. A weakness is the fragmented and non-binding nature of the current frameworks, which may not provide full legal certainty.
- **International Alignment:** The UAE actively participates in international AI governance initiatives and aims to align with global standards to enhance its reputation as a hub for AI.

13. United Kingdom



- **Issuing Organization and Mandate:** The UK government, led by the Department for Science, Innovation and Technology (DSIT), to create a «pro-innovation» environment for AI.
- **Legal and Regulatory Approach:** A non-statutory, principles-based framework that leverages existing regulators (like the ICO and Ofcom) rather than a single, new law. A comprehensive AI Bill is anticipated in 2026.
- **Core Principles and Objectives:** The framework is guided by five cross-sector principles: safety, transparency, fairness, accountability, and contestability.
- **Scope and Applicability:** The principles are non-binding and apply across all sectors. Existing regulators are responsible for applying them within their specific domains, such as data protection, competition, and communications.
- **Governance Structure:** A decentralized, sector-led model where existing regulatory bodies interpret and apply the AI principles. The AI Security Institute has also been established to focus on national security and misuse risks.
- **Enforcement Mechanisms:** Enforcement relies on existing legal frameworks and regulators' powers, rather than new AI-specific penalties.
- **Strengths and Weaknesses:** The framework's strength is its flexibility, which allows it to adapt to rapid technological changes. A weakness is the potential for fragmentation and a lack of legal certainty due to the absence of a single, binding law.
- **International Alignment:** Aims to be interoperable and aligns with international standards like ISO/IEC 42001 and the NIST AI RMF. The UK participates in international AI summits to help shape global norms.



14. United States

- **Issuing Organization and Mandate:** The National Institute of Standards and Technology (NIST) and various federal agencies. The primary mandate, as set by a 2023 Executive Order, is to manage AI risks and promote the safe and trustworthy development of AI.
- **Legal and Regulatory Approach:** A decentralized and voluntary approach that combines non-binding frameworks with sector-specific regulations.
- **Core Principles and Objectives:** The NIST AI RMF is based on a structured approach of four core functions: Govern, Map, Measure, and Manage. It emphasizes human-centric values like fairness, transparency, and accountability.
- **Scope and Applicability:** The voluntary framework is applicable to all organizations involved in the AI lifecycle, from developers to users, across all sectors.
- **Governance Structure:** A multi-layered structure that includes federal agencies, state-level legislation, and private-sector initiatives. The NIST provides a foundational resource, while agencies like the Department of Commerce and the Department of Homeland Security are tasked with issuing specific guidance.
- **Enforcement Mechanisms:** Enforcement is voluntary, but some regulations exist at the sectoral or state level. For example, some civil rights laws can be applied to AI systems.
- **Strengths and Weaknesses:** The flexible nature of the frameworks promotes innovation and agility. The main weakness is the lack of a unified, comprehensive legal framework, which can lead to inconsistency and a lack of clear liability.
- **International Alignment:** The U.S. framework is a key reference for international standards. The U.S. and UK have a joint initiative on responsible AI testing and assurance.

International Entities

OECD AI Management Framework

1. Issuing Organization / Country/ Year of Release and Updates

The OECD AI Management Framework, formally known as the OECD Recommendation on Artificial Intelligence, was issued by the Organization for Economic Co-operation and Development (OECD). This intergovernmental body includes 38 member countries and collaborates with many others globally. While headquartered in Paris, the framework was developed through international, multi-stakeholder consultation. The framework was initially released in May 2019, marking the first intergovernmental standard on AI. It was updated in May 2024 to address recent technological advancements, such as generative AI, and emerging challenges like misinformation, algorithmic safety, and intellectual property.

The OECD has also an ONE AI is an informal advisory network of experts from governments, civil society, academia, private sector, and technical domains. Its role is to provide AI specific policy advice to the OECD on digital economy and AI topics. It supports the OECD's AI work by contributing to the OECD.AI Policy Observatory and facilitating information exchange and collaboration between OECD and other international AI initiatives & organizations. The network helps design implementation guidance to operationalize the OECD AI Principles. It helps identify synergies across global AI initiatives and raises issues of international cooperation for trustworthy AI. The network also interacts with AIGO (the OECD's Working Party on AI Governance), providing advisory input.

The OECD's Digital Policy Committee has a Working Party on Artificial Intelligence Governance (AIGO). AIGO "oversees and gives direction to the DPC work program on AI policy and governance." Its activities include: Analysis of design, implementation, monitoring, and evaluation of national AI policies and action plans; Oversight of AI impact assessments and approaches for trustworthy, accountable AI; Supervising measurement and data efforts via the OECD.AI Observatory; Conducting foresight work on AI and related emerging technologies; Engaging in outreach to non-OECD countries to support adoption of OECD AI standards. AIGO is non binding: it issues guidance, tools, and policy frameworks, but does not itself enforce regulation.

2. Main Objectives

The OECD's recommendation aims to ensure that AI development is innovative, trustworthy, and respects human rights and democratic values. It serves as a values-based foundation to guide policy, promote responsible innovation, mitigate risks, and foster international cooperation. It also provides a shared language and conceptual foundation for national and sectoral AI strategies.

3. Legal and Regulatory Approach

The OECD AI Principles are voluntary and non-binding. They are issued as a Council Recommendation, meaning countries adhere to them voluntarily.

The framework does not prescribe binding regulations. Instead, it encourages countries/companies to adopt these high-level principles into their own regulatory or policy systems. It is a soft law instrument that shapes national policies and fosters policy interoperability, rather than acting as a direct regulatory tool.

4. Core Principles

The OECD framework contains two sets of principles:

a. Values-based Principles (for all AI actors):

- Inclusive growth, sustainable development, and well-being
- Human-centered values and fairness (including respect for human rights, non-discrimination, and rule of law)
- Transparency and explainability
- Robustness, security, and safety
- Accountability of AI actors

b. Recommendations for Policymakers:

- Invest in AI research and development.
- Foster a digital ecosystem for AI.
- Shape an enabling policy environment.
- Build human capacity and prepare for labor market transitions.
- Promote international cooperation for trustworthy AI.

5. Scope

The framework has a broad scope, applying to the private and public sectors, to all AI systems and actors (developers, deployers, users) across the entire AI lifecycle — from design and development to deployment and use. It applies across sectors and technologies, including newer domains such as general-purpose and generative AI, especially following the 2024 update. It is intended for global application, including both OECD and non-OECD countries.

6. Accompanying Documents / Guidelines

Supporting materials include the OECD.AI Policy Observatory, which hosts data, metrics, best practices, and tools for implementation. Other documents include:

- The full text of the OECD Recommendation on AI
- Reports on implementation progress
- A 2024 update report outlining changes for innovative technologies.
- Working papers and country profiles that map national policies to OECD principles.
- Technical definitions (e.g., of “AI system,” “AI lifecycle,” “AI actors”)

7. Dependencies

- Political will to integrate OECD principles into national laws and policies.
- Government capacity (technical expertise, regulatory institutions, funding)
- National AI strategies aligned with OECD principles.
- Legislative alignment (e.g., data protection laws, algorithmic accountability)
- OECD stresses inclusive implementation, requiring action from government, private sector, academia, civil society, and international organizations.
- Engagement of tech companies in developing transparent and accountable AI
- Collaboration with academics and researchers for responsible innovation
- Civil society oversight and advocacy to uphold fairness and rights.
- Dialogue platforms like OECD.AI Policy Observatory and GPAI
- Effective implementation requires robust tools, methodologies, and standards to put the principles (e.g., transparency, robustness) into practice.
- Risk assessment frameworks (e.g., impact assessments, audit tools)
- Standards and metrics for AI explainability, fairness, safety (e.g., from ISO, IEEE, NIST)
- Tools for AI system documentation and algorithmic traceability
- Cooperation through multilateral bodies (G7, G20, EU, UN, GPAI)
- Harmonization of legal and ethical standards to avoid regulatory fragmentation
- Cross-border data sharing and AI research collaboration
- Alignment with data protection laws (e.g., GDPR)
- Integration with human rights frameworks
- Coordination with emerging AI regulations (e.g., EU AI Act)
- Use of procurement policies to mandate OECD-aligned AI practices

8. Connection to Other Risk and Ethical Management Initiatives

The OECD AI Principles are widely recognized and connected to several major frameworks:

- The G20 AI Principles are directly based on them.
- They align with EU AI ethics guidelines, the NIST AI Risk Management Framework, the UNESCO AI ethics recommendation, and international standards like ISO/IEC 42001.
- The Hiroshima AI Process (G7-led) builds on these values, particularly in the development of international AI safety norms.
- Many national frameworks (U.S., UK, Canada, etc.) reference the OECD definitions and guidance.

9. Global International Adoption

As of the 2024 update, the framework has been formally adopted by 47 countries, including all OECD members and many non-member partner countries. It serves as a foundational reference for global AI governance, influencing policymaking, risk assessment, and legal reforms in both developed and developing nations. Its broad acceptance makes it a key instrument for international harmonization of AI policy.

UNESCO Recommendation on Ethics of Artificial Intelligence:

1. Issuing Organization / Country/ year of release and updates

This framework is issued by UNESCO — the United Nations Educational, Scientific and Cultural Organization. It's a global UN body headquartered in Paris, France. It was adopted by UNESCO's General Conference, representing its Member States.

The Recommendation was adopted on 23 November 2021 at UNESCO's 41st General Conference in Paris. As of now, there is no publicly known comprehensive update of the full Recommendation text. However, UNESCO has developed supporting instruments since then (e.g., Ethical Impact Assessment tool, Readiness Assessment Methodology).

2. Main Objectives

The main objectives of UNESCO's Recommendation are:

To provide a universal framework of values, principles and actions that guides States in formulating legislation, policies, or other instruments about AI, consistent with international law.

- To guide actions of individuals, communities, institutions, and private companies so that ethics is embedded throughout the AI system lifecycle.

- To protect, promote and respect human rights and fundamental freedoms, human dignity, equality (including gender equality), environmental sustainability, and cultural diversity.
- To foster peaceful, just, interconnected societies and ensure that AI systems work for the common good rather than exacerbating inequalities or harms.

3. Legal and regulatory Approach (Mandatory vs. Voluntary)

- The Recommendation is voluntary. It is a normative instrument but not a binding treaty. The text recommends that States take “appropriate steps, including whatever legislative or other measures may be required ... in conformity with the constitutional practice ... to give effect within their jurisdictions...” meaning States may choose how to implement it according to their legal systems.
- Because it is nonbinding, its regulatory force is indirect: it influences national laws, policies, regulations, guidelines rather than itself imposing legal obligations.
- It provides detailed policy action areas so that governments can build regulatory or oversight mechanisms (e.g., impact assessments, data protection, oversight, transparency).
- It encourages multistakeholder governance, adaptive and inclusive regulation, oversight, and redress mechanisms.

4. Core Principles

UNESCO’s framework is built on values and principles, which are to guide ethical AI systems. Some of the central values include:

Human rights and human dignity

- Living in peaceful, just, and interconnected societies
- Ensuring diversity and inclusiveness
- Environment and ecosystem flourishing

The ethical principles (ten core principles) include:

- Proportionality and “Do No Harm”
- Safety & Security
- Right to Privacy & Data Protection
- Multistakeholder and Adaptive Governance & Collaboration
- Responsibility and Accountability (auditability, traceability, oversight)
- Transparency and Explainability (as appropriate to context)
- Human Oversight and Determination
- Sustainability (including environmental, ecosystems, SDGs)
- Awareness & Literacy (public understanding, training, media literacy, civic engagement)
- Fairness and NonDiscrimination

5. Scope

- The Recommendation addresses ethical issues throughout the entire AI system lifecycle: research, design, development, deployment, use, maintenance, evaluation, and termination.
- It is intended for all AI actors: governments (Member States), private sector, academia, civil society, technical actors.
- The Recommendation is global: every UNESCO Member State is part of it (193 Member States).
- The domain covers the sectors that fall within UNESCO's mandate: education, science, culture, communication, and information; but also, broader ramifications on environment, health, etc.

6. Accompanying Documents / Guidelines

- Ethical Impact Assessment (EIA) tool: to help assess whether specific AI systems are aligned with the values/principles and to ensure transparency.
- Readiness Assessment Methodology (RAM): to help Member States evaluate how well prepared they are to implement the Recommendation.
- UNESCO also offers capacitybuilding materials, good practices repositories, policy guidance, and stakeholder engagement platforms.
- The inclusion of readiness assessment helps with adapting to different levels of capacity.
- Sectors and contexts outside UNESCO's direct domain (for example, defense, frontier AI, etc.) may require additional adaptation or supplementary regulation.

7. Dependencies

- Requires legal systems that can translate values and principles into laws / regulations when needed (e.g., privacy laws, data protection, oversight mechanisms).
- Human capacity: expertise in ethics, AI technicalities, regulation, impact assessment.
- Institutional capacity: governance bodies, oversight, audit, judicial or regulatory frameworks.
- Resources: financial, technical, infrastructural support. Especially for low and middleincome countries.
- Cultural / societal acceptance: public awareness, literacy, participation are needed.

8. Connection to Other Risk & Ethical Management Initiatives

- Links to international human rights law: the Recommendation explicitly anchors itself in international law and UN human rights obligations.
- Overlaps with frameworks like OECD AI Principles, EU AI ethics guidelines, risk management frameworks in other regions. Many of the same values (accountability, fairness, transparency, safety).
- UNESCO's Recommendation helps fill gaps in global ethics includes environment/ecosystems explicitly, literacy, cultural diversity.
- Also intersects with the UN's Sustainable Development Goals (SDGs).

9. Global / International Adoption

- Adoptability is high in principle; because it allows voluntary, contextsensitive implementation, countries can adopt gradually.
- The availability of tools like RAM and EIA aids adoptability.
- The Recommendation has been adopted by all 193 UNESCO Member States, making it truly global in formal adoption.
- Many countries refer to it when crafting their national AI ethics or policy strategies.
- It also serves as an international benchmark or reference for civil society, research institutions, private sector actors in many parts of the world.

Hiroshima AI Process: Detailed Overview

1. Issuing Organization / Countries/ year of release and updates

The Hiroshima AI Process is a G7 initiative (Group of Seven: Canada, France, Germany, Italy, Japan, United Kingdom, United States, plus the European Union participating) under Japan's presidency (2023). It involves cooperation with international bodies like the OECD and the Global Partnership on AI (GPAI).

The Process was launched in May 2023 at the G7 Summit in Hiroshima. On October 30, 2023, the G7 adopted "the International Guiding Principles and International Code of Conduct for Organizations Developing Advanced AI Systems". Updates and companion mechanisms (like a reporting framework) have been developed: e.g., a pilot for monitoring the application of the Code of Conduct in mid2024, and a finalized reporting framework by end2024 / early 2025.

2. Main Objectives

- To promote safe, secure, and trustworthy AI, especially for advanced AI systems (foundation models, generative AI).
- To manage risks to individuals, society, democratic values, human rights, while harnessing transformational opportunities.
- To foster international cooperation, transparency, accountability, and harmonization / interoperability of governance across jurisdictions.
- To develop a Comprehensive Policy Framework that includes guidelines, codes of conduct, monitoring, and projectbased cooperation.

3. Legal and regulatory Approach (Mandatory vs. Voluntary)

The Hiroshima AI Process is voluntary / nonbinding for organizations. The Code of Conduct and Guiding Principles are not statutes or laws; they are intended to be commitments by organizations, not legal obligations. It uses a softlaw approach: voluntary principles, codes, reporting frameworks, riskbased guidance. It Emphasizes riskbased regulation: organizations are asked to follow actions “commensurate to the risks” associated with advanced AI systems and projectbased cooperation and multistakeholder processes as part of regulatory shaping. It is intended to inform future regulation rather than itself being regulation.

4. Core Principles / Actions

The Process has two main elements: Guiding Principles and Code of Conduct. Guiding Principles (International Guiding Principles for Organizations Developing Advanced AI Systems): These are high level values and norms intended to apply to all stages of advanced AI systems (design, development, deployment, use) and to all AI actors. Code of Conduct (Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems): It spells out 11 Actions (detailed commitments) for organizations. Some of these include:

- Identifying, evaluating, mitigating risks throughout the AI lifecycle, including via redteaming, traceability etc.
- Monitoring for vulnerabilities, misuse after deployment; incidents management.
- Transparent reporting of capabilities, limitations, performance, safety / societal risk assessments.
- Responsible information sharing; collaborating across organizations.
- Having internal governance & risk management policies; ensuring privacy, security, intellectual property protection.
- Investing in security controls, provenance (like watermarking or content authentication), research for mitigation, addressing global challenges (like climate, health, education).

5. Scope

- Applies to organizations developing advanced AI systems, especially foundation models and generative AI. Also includes actors from private sector, academia, civil society, public sector where relevant.
- Covers the entire AI lifecycle: design, development, deployment, use, including postdeployment risks.
- The geographic scope initially is the G7 plus EU; but it aims to have wider adoption via outreach, inclusive multistakeholder consultation, and the “Friends Group” of the Hiroshima AI Process involving additional countries / regions.

6. Accompanying Documents / Guidelines

- The International Guiding Principles document.
- The International Code of Conduct document (11 Actions etc.).
- A reporting framework developed by OECD to monitor organizations’ alignment with the Code of Conduct. Pilot launched in 2024; fully finalized in late 2024/early 2025.
- Projectbased cooperation initiatives (e.g., content authentication / labeling of AIgenerated content).

7. Dependencies

- Depend on institutional capacity: organizations need riskmanagement capability, technical expertise, governance structures.
- Depend on trust and collaboration among organizations to share data, vulnerabilities, adhere to reporting.
- Depend on monitoring infrastructure: organizations need to report, governments or international bodies need to collect, compare and use the data.
- Depend on alignment with legal frameworks: privacy law, intellectual property law, human rights law.

8. Connection to Other Risk & Ethical Management Initiatives

- Builds on OECD AI Principles. The Hiroshima Process explicitly references and aligns with those principles.
- Has parallels with other frameworks like the EU AI Act, the NIST AI Risk Management Framework, etc., particularly around high risk / advanced AI systems.
- It complements or overlaps with other international initiatives (GPAI, standardization bodies).
- It is part of the growing “soft law / voluntary codes + reporting + then regulation” incremental model in AI governance.

9. Global / International Adoption

- Adoption among major AI developers seems underway; some companies have already pledged to report under the reporting framework.
- The design of a reporting framework makes it easier for organizations to align practices with the Code. Doing so voluntarily is easier politically than being forced.
- But for full adoption (especially outside G7, or in smaller or less-resourced institutions), challenges remain (cost, capacity, legal alignment).
- Initially G7 + EU, but through “Friends of HAIP” group there are many more countries / regions expressing interest in adopting or aligning with the Process. According to a report, 49 countries/regions supported the “Friends Group” as of early 2024.

Global Partnership on Artificial Intelligence (GPAI) — Detailed Overview

1. Issuing Organization / Country/ year of release and updates

The Global Partnership on Artificial Intelligence (GPAI) is a multi-stakeholder international initiative involving governments, industry, academia, civil society, and international organizations. It was co-founded by Canada and France and is hosted by the OECD. GPAI was launched in June 2020. It began with 15 founding members and has grown to about 29 member countries/regions as of mid-2024. In July 2024, GPAI integrated more closely with the OECD, enhancing its international reach and coordination.

2. Main Objectives

- Bridge the gap between AI theory and practice through applied research and pilot projects.
- Promote trustworthy, human-centric, safe, and secure AI aligned with democratic values, human rights, inclusion, fairness, and innovation.
- Foster international cooperation to avoid duplication, share best practices, and provide a global reference point on AI issues.
- Address AI’s societal impacts in domains like environment, public policy, and future of work.

3. Legal and Regulatory Approach (Mandatory vs Voluntary)

- GPAI is voluntary and non-binding. It does not impose legal obligations on its members but provides a platform for collaboration, research, and policy guidance.
- It complements, rather than replaces, national and international regulatory efforts.
- Its work produces research, policy recommendations, frameworks, and tools that governments and organizations can use to inform their own regulatory decisions.
- Importantly, GPAI's outputs support regulatory efforts like the EU AI Act and the EU GPAI Code of Practice. The EU GPAI Code of Practice complements the EU AI Act by providing guidelines on responsible AI deployment, emphasizing transparency, risk management, and accountability aligned with EU legislation.

4. Core Principles

- Inclusive growth, sustainable development, and well-being.
- Human-centered values and fairness, including respect for human rights and non-discrimination.
- Transparency and explainability.
- Robustness, security, and safety.
- Accountability.

5. Scope

- Private and public sectors: GPAI covers AI systems broadly, across sectors and applications, including data governance, environment, public policy, and the future of work.
- It addresses the full AI lifecycle but excludes defense and state security applications.
- Members span many continents, including OECD countries and partners beyond OECD membership.

6. Accompanying Documents / Guidelines / Tools

- Data Governance Working Group Framework Paper
- Reports on algorithmic transparency in the public sector.
- The Responsible AI Strategy for the Environment (RAISE) initiative.
- Checklists, policy briefs, and best practice documents for data sharing and governance.
- Ministerial Declarations that set strategic priorities.
- The EU GPAI Code of Practice, which provides practical voluntary guidance to align AI development with EU regulation and ethical standards.

7. Dependencies

- Political will and commitment from member states.
- Technical and regulatory capacity.
- Collaborative trust among stakeholders.
- Up-to-date knowledge of AI technologies.
- Complementary legal frameworks in privacy, security, and human rights.
- Sustainable funding and institutional continuity.

8. Connection to Other Risk and Ethical Management Initiatives

- Built around and aligned with OECD AI Principles.
- Complementary to regulatory frameworks like the EU AI Act and related EU GPAI Code of Practice, which provide enforceable regulation and voluntary best practices, respectively.
- Supports UNESCO’s ethical AI frameworks and other national guidelines by translating high-level ethics into actionable tools and policy advice.
- Works as a bridge between ethical principles and practical policy, feeding evidence-based insights into regulation and standards development globally.

9. Global / International Adoption

- High in jurisdictions with political will and institutional readiness.
- Adoption varies with local resources and governance maturity.
- Includes approximately 29 countries and the EU as members as of 2024.
- Widely used as a reference by non-member states and international actors.
- The partnership with the OECD expanded GPAI’s legitimacy and global influence.
- The EU AI Act and the EU GPAI Code of Practice demonstrate how GPAI’s voluntary frameworks can complement and reinforce binding regulatory regimes, enabling broad international impact.

World Economic Forum (WEF) AI Management Framework

1. Issuing Organization / Country/ date of release and updates

The framework is issued by the World Economic Forum (WEF), an international non-governmental organization based in Switzerland, involving business, political, academic, and civil society leaders globally. It is a multi-stakeholder platform rather than a government entity. The WEF has developed multiple AI-related initiatives and frameworks, with major influential publications starting around 2018. Notable AI governance frameworks include the “AI Governance Principles” (2020) and the ongoing “Global AI Action Alliance” (launched 2021). Frameworks and guidance are regularly updated through community consultations and annual meetings.

2. Main Objectives

- To promote responsible and human-centered AI development globally.
- To accelerate cooperation across sectors to ensure AI is developed and deployed safely, inclusively, and ethically.
- To facilitate the development of practical tools, governance frameworks, and policy dialogues to mitigate risks and maximize benefits.
- To foster multi-stakeholder collaboration bridging government, business, academia, and civil society.

3. Legal and regulatory Approach (Mandatory vs Voluntary)

- The WEF's AI frameworks are entirely voluntary and non-binding.
- They serve as guidelines, best practices, and recommendations rather than legal mandates.

Adoption depends on the willingness of organizations, governments, and other stakeholders to implement the principles, as WEF acts as a facilitator of dialogue and norm-building, rather than a regulator. It promotes the creation of shared standards and governance frameworks to inspire consistent AI risk management across sectors and jurisdictions. The WEF collaborates with governments and standard-setting bodies to align with and complement regulatory initiatives like the EU AI Act and OECD AI Principles. It supports multi-sectoral frameworks addressing issues such as AI ethics, transparency, and accountability.

4. Core Principles

WEF's AI governance frameworks emphasize:

- Human-centeredness: AI should respect human rights and dignity.
- Fairness and non-discrimination: Avoiding bias and promoting inclusiveness.
- Transparency and explainability: AI decision-making processes should be understandable.
- Accountability: Clear responsibility for AI impacts.
- Privacy and security: Protecting data and systems against misuse or harm.
- Sustainability: Considering environmental impacts of AI.
- Collaboration: Encouraging cooperation among diverse stakeholders.

5. Scope

- The WEF frameworks cover all AI applications across industries and sectors globally, encompassing the public and private sectors.
- They address the entire AI lifecycle: design, development, deployment, and ongoing management.
- The framework includes social, economic, environmental, and ethical considerations.
- It explicitly encourages multi-sector cooperation including public-private partners.

6. Accompanying Documents / Guidelines / Tools

- AI Governance Principles (2020): Foundational document outlining WEF's AI ethics and governance approach.
- Global AI Action Alliance: A platform for collaborative projects and development of tools to implement AI governance.
- Toolkit for Responsible AI: Practical guides and frameworks for businesses to assess and manage AI risks.
- Reports on AI's impact on the future of work, environment, and society.
- Model AI governance frameworks developed with partners to support policy and organizational implementation.

7. Dependencies

- Requires ongoing stakeholder commitment and collaboration.
- Dependent on political will and resource availability among governments and companies.
- Success depends on integration with existing and emerging legal frameworks and standards.
- Needs continuous updating to keep pace with AI technological advances.

8. Connection to Other Risk and Ethical Management Initiatives

- Closely aligned with OECD AI Principles and complements UNESCO's AI Ethics Recommendation.
- Supports and works alongside regulatory frameworks such as the EU AI Act by providing industry input and implementation guidance.
- Engages with initiatives like the Partnership on AI (PAI) and GPAI to foster harmonized approaches.
- Facilitates global dialogue bridging diverse regulatory, ethical, and technical frameworks to reduce fragmentation.

9. Global / International Adoption

- High adoptability among multinational corporations, governments, and international organizations familiar with WEF processes.
- Effective as a platform for shaping voluntary best practices and guiding emerging regulatory frameworks.
- May face adoption challenges in jurisdictions with limited resources or where digital governance is nascent.
- WEF's AI governance frameworks have been widely cited and used by major global corporations, governments, and international bodies.
- The Global AI Action Alliance includes participants from over 80 countries and numerous organizations, reflecting broad international buy-in.
- While voluntary, WEF's frameworks influence emerging national AI policies and global standard-setting efforts.

International Telecommunication Union (ITU) AI Management Framework — Detailed Overview

1. Issuing Organization / Country/ release date and updates

The International Telecommunication Union (ITU) is a United Nations specialized agency based in Switzerland. It facilitates global cooperation and standardization in information and communication technologies (ICTs), including AI.

The AI for Good Global Summit was launched in 2017 as a flagship event to explore AI's positive social impact. ITU's Focus Group on Artificial Intelligence for Health (FG-AI4H) was established in 2018 and led to ongoing standardization efforts. Continuous updates through ITU's standardization activities, notably in the ITU-T Study Group 16 on multimedia coding and AI applications.

2. Main Objectives

- Facilitate the development of global AI standards and best practices ensuring interoperability, safety, and trustworthiness.
- Promote AI for social good and sustainable development goals (SDGs).
- Enable international cooperation among governments, industry, and academia on AI policy, ethics, and technology.
- Provide a platform for inclusive dialogue on AI governance, bridging developed and developing countries.
- Support regulatory frameworks and risk management in ICT and AI contexts.

3. Legal and regulatory Approach (Mandatory vs Voluntary)

- ITU develops technical standards and recommendations, which are voluntary but widely adopted by member states and industry.
- It does not have enforcement powers but influences national regulations through standard-setting and policy advice.

Facilitates capacity building for regulators, especially in developing countries.

4. Core Principles

- **Interoperability** and standardization to enable global AI system compatibility.
- **Safety, security, and privacy** in AI deployment.
- **Inclusivity and accessibility** to bridge the digital divide.
- **Ethical AI** aligned with human rights and sustainable development.
- **Transparency and accountability** in AI systems.
- Encouragement of **innovation balanced with risk management**.

5. Scope

- Focus on AI as it relates to ICTs and telecommunications infrastructure for the public and private sectors alike.
- Covers AI applications in health, environment, smart cities, digital inclusion, and more.
- Targets both technical standards (e.g., data formats, AI system evaluation) and policy frameworks.

6. Accompanying Documents / Guidelines / Tools

- ITU-T Recommendations, including AI-focused standards like Y.3172 (Architectural framework for AI systems in future networks).
- Reports and guidelines from the AI for Good Global Summit series.
- Focus Group AI for Health (FG-AI4H) guidelines on AI in healthcare.
- Policy briefs and capacity-building toolkits for regulators.
- Collaborative frameworks with ISO/IEC on AI standards (e.g., JTC 1/SC 42).

7. Dependencies

- Collaboration with other standards bodies (ISO, IEC).
- Political support from member states for adopting standards and policies.
- Continuous technological monitoring and expert contributions.
- Adequate resources for capacity-building and outreach.

8. Connection to Other Risk and Ethical Management Initiatives

- Coordinates with ISO/IEC JTC 1/SC 42 AI standards committee to ensure technical and ethical standards alignment.
- Aligns with OECD AI Principles, UNESCO's AI Ethics Recommendation, and other international guidelines.
- Interfaces with regional regulatory frameworks like the EU AI Act by promoting interoperable standards.
- Works alongside WHO on AI in health (through FG-AI4H).
- Promotes convergence of AI governance across technical, ethical, and policy dimensions.

9. Global / International Adoption

As a UN specialized agency with near-universal membership, ITU standards have broad international recognition and uptake and enjoys high adoptability by telecom operators, governments, and regulators seeking alignment with international standards. The AI for Good Summit attracts global stakeholders from governments, industry, and civil society. ITU standards are increasingly referenced in national AI strategies and international AI governance efforts.

Plays a key role in capacity building and knowledge transfer to developing and least developed countries, enabling global AI inclusiveness.

BRICS AI Management Framework

1. Issuing Organization / Country/ release date and updates

- BRICS is an intergovernmental organization comprising ten countries: Brazil, Russia, India, China, South Africa, Egypt, Ethiopia, Indonesia, Iran and the United Arab Emirates.
- AI governance efforts stem from BRICS Joint Statements and collaborative initiatives, led by respective national agencies and ministries.
- There is no centralized BRICS AI management body, but coordination happens through annual summits and working groups.

AI-related collaboration in BRICS has evolved over the past 5-7 years, with more concrete joint declarations emerging since around 2018. The BRICS Digital Economy Ministerial Meetings have increasingly focused on AI and digital governance since 2019-2020.

- The BRICS AI Working Group was established more formally around 2021-2022, fostering cooperation.
- Updates tend to follow annual or biannual summits, with the latest joint statements emerging in 2023-2024.

2. Main Objectives

- Promote collaborative AI research, development, and innovation within BRICS countries.
- Ensure AI development supports sustainable development, economic growth, and social welfare.
- Foster data sharing, interoperability, and mutual regulatory understanding among BRICS nations.
- Enhance digital sovereignty and cybersecurity in AI deployment.
- Encourage ethical AI use respecting cultural and national contexts, balancing innovation with risk mitigation.
- Strengthen global south perspectives and reduce technological dependencies on developed economies.

3. Legal and regulatory Approach (Mandatory vs Voluntary)

- The BRICS AI approach is primarily voluntary and consensus-based within the bloc.
- Cooperation focuses on soft law instruments such as joint declarations, memoranda of understanding, and guidelines.
- Emphasizes coordination of national AI regulatory regimes rather than harmonization or supranational enforcement.

- Focus on risk management and responsible innovation with attention to country-specific priorities.
- Encourages capacity building and technical exchanges to strengthen regulatory frameworks domestically.

4. Core Principles

- Sovereignty and respect for national legal frameworks.
- Ethical AI respecting human rights, fairness, and non-discrimination.
- Transparency and accountability in AI systems.
- Security and privacy protection, especially in data governance.
- Sustainable and inclusive AI innovation.
- Collaboration for equitable global AI development.
- Digital sovereignty emphasizing local control over AI technologies and data.

5. Scope

- Relevant to the Public and private sectors and covers AI research, development, deployment, and governance across economic, social, and technological domains relevant to BRICS countries.
- Addresses data governance, AI standards, digital infrastructure, cybersecurity, and capacity building.
- Focuses on AI applications aligned with national development goals and SDGs.
- Excludes military or defense AI applications from collective governance discussions.

6. Accompanying Documents / Guidelines / Tools

- BRICS Joint Statements on Digital Economy and AI (various years from 2019 onwards).
- Reports from BRICS AI Working Group meetings outlining cooperation roadmaps.
- Memoranda of Understanding (MOUs) between member countries on AI research collaboration.
- Technical cooperation frameworks focusing on AI standardization and interoperability.
- National AI strategies of individual BRICS countries referenced in cooperation.

7. Dependencies

- Political will and mutual trust among BRICS member states.
- Coordination mechanisms such as the AI Working Group functioning effectively.
- National capacity in AI research, regulation, and infrastructure.
- Cooperation with external organizations and standards bodies (e.g., ISO, ITU).
- Alignment with global AI governance trends while maintaining sovereignty.

8. Connection to Other Risk and Ethical Management Initiatives

- BRICS AI cooperation references OECD AI Principles and UNESCO's AI Ethics Recommendation as global benchmarks.
- Engages in dialogue with international AI initiatives including GPAI and ITU.
- Reflects an interest in developing alternative models to Western AI governance frameworks, emphasizing sovereignty and development.
- Encourages alignment with regional regulatory developments (e.g., China's AI regulations, India's national AI strategy).

9. Global / International Adoption

- BRICS AI cooperation primarily focuses on internal collaboration but has growing visibility in global AI governance forums.
- Serves as an important voice for the Global South in international AI policy discussions.
- BRICS joint AI positions influence UN AI-related debates and forums such as AI for Good (ITU) and the UNESCO AI Ethics process.

G20

1. Issuing Organization / Country/ Date of release and updates

The framework is issued by the G20 (Group of Twenty), an international forum of 19 countries plus the European Union. The principles are adopted in G20 Ministerial meetings and Leaders' Declarations. The G20 does not belong to a single country; its presidency rotates among members.

The G20 first adopted its AI Principles in June 2019, during the G20 Digital Economy Ministers' Meeting in Tsukuba, Japan.

- The G20 continues to include AI in its agenda; recent years (2023-2025) under various presidencies (India, Brazil, South Africa) have built on or reaffirmed those principles in new declarations and working group initiatives.

2. Main Objectives

- To commit G20 members to responsible, trustworthy, humancentered AI that supports inclusive growth, social welfare, and sustainable development.
- To provide a common set of ethical principles and policy guidance for AI actors (governments, developers, deployers) to manage AI risks, especially around fairness, transparency, accountability, safety, data protection.
- To encourage international cooperation, capacity building, research & innovation in AI among member states.

3. Legal and regulatory Approach (Mandatory vs. Voluntary)

- The G20 AI Principles are nonbinding / voluntary. They are political commitments rather than legal obligations.
- The G20 approach is soft law / policy guidance, not regulation. It provides highlevel principles and recommendations for national policies.
- It encourages working groups and ministerial cooperation, sharing of best practices, and alignment of national AI strategies.
- Recently, G20 has set up a Task Force on “AI, Data Governance, and Innovation for Sustainable Development” under its 2025 South African presidency to deepen collaborative governance.

4. Core Principles

The 2019 G20 AI Principles are drawn from the OECD AI Principles. Key core principles include:

- Inclusive growth, sustainable development and wellbeing, including reducing inequality and ensuring underrepresented populations benefit.
- Humancentered values and fairness: respect for rule of law, human rights, democratic values, privacy, nondiscrimination, social justice.
- Transparency and explainability, including meaningful disclosure appropriate to context.
- Robustness, security, and safety across the AI lifecycle, with risk management and traceability.
- Accountability: AI actors are accountable for respecting the above and ensuring outcomes are lawful and ethical.
- Additionally, the G20 AI Principles include policy recommendations for governments, such as investing in research & development; fostering ecosystems; shaping enabling policy environments; capacity building; international cooperation.

5. Scope

- Applies to the private and public sectors, to all G20 member countries, and is intended to guide all “AI actors” (developers, users, governments) within those countries.
- Covers the full AI lifecycle, from design, development, deployment, use, to oversight and risk mitigation.
- Encompasses multiple sectors and usecases: digital economy, health, education, environment etc. AI is treated as horizontal (crosscutting) rather than sectorspecific.

6. Accompanying Documents / Guidelines / Tools

- The original G20 “Principles for responsible stewardship of Trustworthy AI” document (part of 2019 Ministerial meeting materials) is the core text.
- Subsequent declarations, Leaders’ Declarations (e.g., 2023, 2024, 2025) reaffirming or expanding these principles with additional focus areas.
- Working group outputs: e.g., G20 Digital Economy Working Group; the Task Force on AI, Data Governance, and Innovation for Sustainable Development established in 2025.
- Some associated policy documents and statements around information integrity, digital inclusion, data protection etc.

7. Dependencies

Depend on national regulatory and legal systems being willing and able to incorporate principles (privacy laws, data protection, human rights law etc.).

- Depend on technical capacity (for developers, government oversight, auditing).
- Depend on political stability and consensus among G20 members.
- Depend on resources (funding, institutions) for implementing policy, capacity building, monitoring.
- Depend on keeping pace with fast advances in AI (frontier models, generative AI etc.), so that the principles remain relevant and updated.

8. Connection to Other Risk and Ethical Management Initiatives

- The G20 AI Principles are explicitly drawn from the OECD AI Principles (2019).
- They align with and are reinforced by other frameworks such as UNESCO’s AI Ethics Recommendation, ISO/IEC AI standards, GPAI, the Hiroshima AI Process, and national AI regulations.
- G20 also interacts via its working groups with issues of digital economy, data governance, and innovation, overlapping with privacy, data protection, digital inclusion, etc.

- Current G20 declarations include references to information integrity, algorithmic transparency and explainability, nondiscrimination — consistent with global risk / ethical management initiatives.

9. Global / International Adoption

- Among G20 members, the principles are formally endorsed and periodically reaffirmed in Leaders' Declarations.
- The G20 also influences nonmember countries and global governance by virtue of being a major economy grouping; its principles serve as persuasive norms globally.
- Many nonG20 states and organizations refer to G20 AI Principles as benchmarks in their own AI policy development. However, for nonG20 or developing countries, adoptability may require technical, financial, institutional support.
- Through the Task Force (2025) and working groups, G20 aims to deepen international coordination (e.g., AI for Africa and sustainable development) which expands influence and adoption.

International Network of AI Safety Institutes

1. Issuing Organization / Country / Year of Release and Updates

- Launched on November 2021, 2024 in San Francisco.
- Founding members are technical AI safety institutes (or equivalent governmentmandated safety/scientific offices) from: Australia, Canada, the European Commission, France, Japan, Kenya, the Republic of Korea, Singapore, the United Kingdom, and the United States.
- The launch affirmed and built upon the Seoul Statement of Intent toward International Cooperation on AI Safety Science, which was released on May 21, 2024.

2. Main Objectives

- To advance research on risks and capabilities of advanced (or frontier) AI systems; share results.
- To build common practices for testing such systems; including joint testing exercises and sharing domestic evaluation results.
- To facilitate shared guidance: interpreting tests of advanced systems, building interoperable technical understanding.
- To promote inclusion: engaging partners globally at different levels of development; sharing technical tools and information in accessible ways.

3. Legal and Regulatory Approach (Mandatory vs Voluntary)

- The Network is voluntary; membership does not impose binding legal obligations.
- It is technical / scientific in focus, not a regulatory or enforcement body. Its role is cooperation, research, technical alignment—not regulation.

4. Core Principles

- Emphasis on scientific rigor in understanding risks and capabilities.
- Interoperability & shared technical understanding across members.
- Inclusivity: linguistic, cultural diversity, varied country development levels.
- Transparency and shared best practices in testing, risk evaluation.

5. Scope

- Focus is on advanced AI systems—foundation models, future frontier risks, synthetic content risk, etc.
- Members are all from public or quasi-public technical / scientific organizations.
- Global in membership, though initial membership is limited to those listed above. Scope includes sharing knowledge, testing, guidance, inclusion.

6. Accompanying Documents / Guidelines / Tools

- Mission Statement document (Nov 21, 2024) laying out priority areas: research, testing, guidance, inclusion.
- Fact Sheet by U.S. Department of Commerce / State with details on funding commitments (>\$11M for synthetic content research) and priority technical focus areas (synthetic content risks, testing foundation models, advanced risk assessment).
- Joint statement on risk assessments of advanced AI systems outlining shared aspects (actionable, transparent, reproducible, etc.).

7. Dependencies

- Requires technical capacity to do advanced AI safety research and testing.
- Funding commitment: e.g., the > US\$11M around synthetic content research.
- Shared standards / methodologies for testing, evaluation.

8. Connection to Other Risk and Ethical Management Initiatives

- Builds on the Seoul Statement of Intent on AI Safety Science.
- Aligns with broader safety, risk assessment, and frontier AI governance conversations (e.g., Bletchley Declaration, AI Action Summits).

9. Global / International Adoption / Impact

- Initial global membership across multiple continents, including Africa (Kenya).
- Early funding commitments showing real resource allocation (synthetic content risk work).
- Has begun joint testing exercises and shared evaluation plans among members.

Regional Entities

Latin America and Caribbean Regional Council on the Ethics of AI

1. Issuing Organization / Country / Year of Release and Updates

- Latin America and Caribbean Regional Council on the Ethics of AI is a regional collaborative platform, not a formalized treaty or globally recognized institutional framework like UNESCO.
- Public documentation on the Council is limited. No official “founding document” or formal treaty exists.
- Regional AI ethics initiatives exist (e.g., regional meetings, networks), but no single formalized council with binding authority or regular updates has been broadly publicized.
- The Council is a voluntary consultative network formed around 2020-2023.

2. Main Objectives

- Regional initiatives like those by CEPAL (Economic Commission for Latin America and the Caribbean) and others emphasize ethical AI aligned with human rights, inclusion, and regional development goals.
- Public documents from regional forums highlight objectives like those listed: promoting ethical AI, fostering collaboration, protecting rights, and capacity building.
- The Council’s objectives are consistent with regional priorities but are not consolidated in a single official document.

3. Legal and Regulatory Approach (Mandatory vs. Voluntary)

- Latin America and Caribbean countries typically adopt voluntary guidelines and recommendations on AI ethics, with some diversity.
- No evidence of regional binding legislation or mandatory enforcement mechanisms through this Council.

4. Core Principles (Values + Ethical Principles)

- Regional reports and policy papers (from CEPAL, regional AI ethics forums, and the Organization of American States) emphasize:
 - Human rights and dignity
 - Social justice and inclusion
 - Cultural diversity (including Indigenous rights)
 - Environmental sustainability
 - Transparency, accountability, fairness

5. Scope

- Regional initiatives promote a full AI lifecycle approach in policy discussions (research to deployment).
- Sectors like education, healthcare, governance, environment are emphasized due to their regional relevance.
- Stakeholders targeted include governments, academia, civil society, private sector.

6. Accompanying Documents / Guidelines

- No formal regional AI ethics toolkits or mandatory guidelines exist under the Council.

7. Dependencies

- Implementation depends heavily on:
 - National legal frameworks (varies widely)
 - Technical and institutional capacity (some countries more advanced than others)
 - Resource availability and public awareness
- Dependencies identified align with existing regional capacity challenges.

8. Connection to Other Risk & Ethical Management Initiatives

- Latin America and Caribbean regional efforts explicitly reference global frameworks, including:
 - UNESCO's Recommendation on Ethics of AI
 - UN SDGs
 - OECD AI Principles
 - Regional human rights frameworks
- Many countries refer to UNESCO's guidelines when shaping national AI ethics policies.

9. Global / International Adoption

- The Council has no formal global enforcement or adoption mechanism.
- Adoption of ethical AI principles and frameworks happens at the national level, with the Council acting as a facilitator or knowledge-sharing platform.

The African Region – AI Ethics and Governance Overview

1. Issuing Organization / Country / Year of Release and Updates

- **Issuing Organization:** African Union (AU)
- **Document:** Continental Artificial Intelligence Strategy for Africa
- **Year of Release:** 2024 (endorsed July 2024)
- **Updates:** Strategy is recent; no major publicized updates yet, but the AU Commission plans continuous development. The strategy is expected to be complemented by An African ethical framework and plan of action.

Complementary efforts include The Smart Africa AI Council is under establishment and is meant to support the implementation the AI Continental strategy. The Council's strategic plan is expected to be submitted during the Transform Africa Summit in July 2025.

The G20's AI initiative for Africa, launched during South Africa's G20 presidency in 2025, is centered around the "AI for Africa" conference held in Cape Town from September 30 to October 1, 2025. This initiative aims to harness artificial intelligence to drive sustainable development and economic growth across the African continent. The initiative is a collaborative effort involving the South African government, the African Union, UNESCO, and leading international development organizations.

2. Main Objectives

- Establish an Africa-centered, inclusive AI ecosystem that reflects African values, cultures, and languages.
- Accelerate development of AI infrastructure, talent, research, and innovation aligned with Africa's socioeconomic needs.
- Support key sectors like education, health, agriculture, infrastructure, peace & security, and governance.
- Promote ethical and responsible AI use that benefits the whole continent and mitigates risks.
- Build human and institutional capacity to govern and manage AI effectively.

3. Legal and Regulatory Approach (Mandatory vs. Voluntary)

- The **Continental AI Strategy is voluntary**.
- It provides **guidance and recommendations**, encouraging AU Member States to develop their own national AI policies and legal frameworks.
- No binding continental AI law or enforcement mechanism exists yet; implementation depends on individual countries' adoption and adaptation.

4. Core Principles (Values + Ethical Principles)

- **Ethical AI use and risk mitigation**
- **Inclusivity and cultural relevance**—preserving African languages, traditions, and identities in AI systems.
- **Human-centered approach**, emphasizing human rights, equity, and social benefit.
- **Sustainability** and alignment with Africa's development goals
- **Collaboration and capacity building** across governments, private sector, and civil society

5. Scope

- Addresses **entire AI lifecycle**: research, design, development, deployment, governance, and evaluation.
- Targets multiple sectors crucial to Africa's development: education, health, agriculture, infrastructure, governance, security.
- Engages all relevant stakeholders: governments, academia, private sector, civil society, technical experts.
- Covers all AU Member States (55 countries across Africa).

6. Accompanying Documents / Guidelines

- AU Commission is developing an **AI Africa Policy** to complement the strategy.
- Some AU member countries have completed their **national AI strategies** or readiness assessments.
- There are **no continent-wide standardized AI ethics tools** like impact assessments or readiness methodologies publicly released yet.
- The strategy complements initiatives like the **African Digital Compact** for digital transformation.

7. Dependencies

Success depends on:

- Strong **national legal frameworks** to translate principles into enforceable laws.
- **Institutional and governance capacity** to regulate and oversee AI technologies.
- **Technical and human resource capacity** for AI development and ethics expertise.
- Adequate **financial and infrastructure resources**, especially for lower-income countries.
- **Public awareness and cultural acceptance** of AI and its ethical implications.

8. Connection to Other Risk & Ethical Management Initiatives

- The strategy aligns with international frameworks such as:
 - UN Sustainable Development Goals (SDGs)
 - Global AI ethics standards (e.g., UNESCO, OECD principles)
- Incorporates uniquely African perspectives on **data sovereignty, decolonization, and communalism** in AI ethics.
- Encourages regional cooperation among AU Member States and with international partners.

9. Global / International Adoption

- The strategy has **continental endorsement by all 55 AU Member States**.
- Adoption is **voluntary and uneven**; some countries actively developing national AI policies, others still in early stages.
- Viewed as a **model for regional AI governance frameworks**, inspiring other continents, or regions.

ASEAN Working Group on AI Governance

1. Issuing Organization / Country / Year of Release and Updates

- **Issuing Organization:** ASEAN (Association of Southeast Asian Nations), through its digital governance bodies, especially the ASEAN Digital Senior Officials Meeting (ADGSOM)/ASEAN Digital Ministers (ADGMIN). The Working Group on AI Governance is chaired by Singapore’s IMDA (Infocomm Media Development Authority).
- **Year of Establishment:**
 - The WG-AI was established in March 2024 at the 1st ASEAN Digital Governments Senior Officials’ Meeting/ATRC Leaders’ Retreat in Phnom Penh. Its mandate was expanded in January 2025 at the 5th ASEAN Digital Ministers’ Meeting.
- **Updates:**
 - In 2024, ASEAN released the ASEAN Guide on AI Governance and Ethics.
 - In January 2025, the “Expanded Guide” was published to address Generative AI (Gen AI) risks and governance.

2. Main Objectives

The WG-AI has several stated objectives:

- To lead and coordinate ASEAN’s regional AI governance agenda, including policy development, regulation, standards, safety, and ecosystem development.
- To create regional frameworks, principles, standards, and best practices for AI.
- To address the governance of generative AI through an expanded guide, identifying and managing risks.
- To facilitate knowledge exchange, research, and capacity building among ASEAN Member States.
- To foster stakeholder engagement (academia, private sector, civil society) and external cooperation with Dialogue Partners (e.g., US, EU, etc.).

3. Legal and Regulatory Approach (Mandatory vs. Voluntary)

- The approach is **voluntary / soft regulatory**. The ASEAN Guide(s) are non-binding recommendations.
- ASEAN does not have centralized legislative power—implementation depends on each Member State adopting, adapting, or aligning national policies with the guide.
- The Guides and WG-AI are intended to support interoperable regional standards, but with flexibility recognizing different levels of readiness among member countries.

4. Core Principles (Values + Ethical Principles)

The ASEAN Guide on AI Governance and Ethics (2024) includes **seven guiding principles**:

- Transparency & Explainability
- Fairness & Equity
- Security & Safety
- Robustness & Reliability
- Human-centricity
- Privacy & Data Governance
- Accountability & Integrity

The Expanded Guide for Generative AI adds risk-related dimensions such as disinformation, deepfakes, bias, IP concerns, etc.

5. Scope

- **Lifecycle Coverage:** The Guides address design, development, deployment, and policy frameworks; the Generative AI expansion specifically focuses on newer risk points.
- **Sectors / Applications:** Focus is on “traditional AI systems” (e.g., rule-based, predictive systems), then expanding to generative AI cases. Use cases are drawn from ASEAN countries.
- **Stakeholders:** Governments (ASEAN Member States), industry, academia, civil society, international partners.
- **Members / Geographic Coverage:** All 10 ASEAN Member States.

6. Accompanying Documents / Guidelines

- **ASEAN Guide on AI Governance and Ethics (2024):** foundational regional guide.
- **Expanded Guide on AI Governance and Ethics — Generative AI (Jan 2025):** supplements the 2024 Guide.
- **ASEAN Responsible AI Roadmap (2025):** mentioned in regional press / documents.
- **AI Ready ASEAN:** an initiative for AI literacy and awareness, to build capacity.

7. Dependencies

- **Readiness Variation:** ASEAN countries have varying levels of AI readiness and infrastructure. Some are advanced, others emerging.
- **Legal & Institutional Capacity:** Member States need legal/regulatory frameworks, agencies, oversight. In many cases these are nascent.
- **Resource Constraints:** Differing resources, technical expertise, data infrastructure, public trust, etc.
- **Stakeholder Participation:** Engaging private sector, academia, civil society required, especially for generative AI risks.

8. Connection to Other Risk & Ethical Management Initiatives

- ASEAN's work aligns with global AI ethics principles and frameworks. The WG-AI cooperates with external partners (UNESCO, etc.) and considers international best practices.
- The ASEAN Digital Masterplan 2025 and other regional digital economy frameworks are connected to the Guide.
- There is push to harmonize with standards emerging globally, especially regarding Gen AI risks.

9. Global / International Adoption / Implementation

- The ASEAN Guide(s) have received endorsement by ASEAN Digital Ministers and are being used as reference points.
- However, actual implementation at national level is varied: some countries already have AI strategies, others are in earlier stages.
- No binding regional enforcement; countries retain full sovereignty.

Arab Region — AI Governance Initiatives

1. Issuing Organization / Year / Updates

- The key bodies: The League of Arab States, the **Arab Information & Communication Technologies Organization (AICTO)**; the **League of Arab States (LAS)** / General Secretariat; national ICT / AI Ministries in various Arab states.
- The Working Group on AI by Arab ICT Ministers (under LAS / AICTO) is a regional cooperative initiative. One of its outputs is the **Arab AI strategy**. And Arab Ethical framework for AI.
- Significant recent events:
 - The AI Initiative by the Secretary General of LAS
 - **Arab Dialogue Roundtable on "Artificial Intelligence in the Arab World: Innovative Applications and Ethical Challenges,"** held 23 February 2025 in Cairo.
 - **Annual Arab Forums on Artificial Intelligence,** 27-28 August 2025, in New Alamein, Egypt, by the Arab Academy for Science, technology and Maritime Transport
- Also, ALECSO adopted a Charter on AI Ethics in June 2025 (Education / Culture / Science domain).

2. Main Objectives

The Arab AI Working Group:

- Developed a common **Arab governance framework** / AI strategy for the region, aligning national-level policies.
- Develop and promote ethically guided AI use: ensuring innovation, but with ethical values, human wellbeing, digital security, trust, digital sovereignty.
- Foster cooperation among member states: sharing best practices, coordinating regulation, aligning on standards.
- Identify & address ethical challenges, risks of AI (in diplomacy, conflict resolution, digital space trust, etc.).
- Support capacity building, infrastructure, projects: e.g., AI incubators, platforms, leadership programs.

3. Legal / Regulatory Approach (Mandatory vs. Voluntary)

- The approach is voluntary / soft governance rather than binding regional legal obligations. At the regional level, alignment is via guidelines, charters, declarations, not mandatory legal enforcement.

4. Core Principles / Values / Ethical Principles

- The strategy Emphasizes the **ethical AI use, humancentered values**, balancing innovation with protection of citizens.
- Respect for **digital sovereignty**: ensuring that the Arab region sets its own values, standards, not wholly imported.
- Inclusion, fairness, social justice, sustainable development.
- Trust, stability, peace: including in diplomacy, conflict resolution.

5. Scope

What the Working Group and related Arab initiatives cover:

- **Lifecycle/Stages**: So far mostly strategy, policy guidance, ethical risk identification, but not all stages like standardized impact assessment, independent oversight uniformly across all states.
- **Sectors**: Includes education, culture, science (via ALECSO), ICT, digital infrastructure; diplomacy, peacekeeping, public service applications.
- **Stakeholders**: Member states' ICT / AI ministries; regional bodies (AICTO, LAS); academia and research institutions; civil society in dialogues; UN/regional partners.
- **Geographic coverage**: Arab League member states; regionwide participation is intended, though degree of engagement varies across countries.

6. Accompanying Documents / Guidelines / Tools / Projects

Key deliverables and tools:

- **Draft Common Arab AI Strategy:** the Working Group has produced or is producing a draft version.
- **Arab Ethical Framework (to be adopted)**
ALECSO Charter on AI Ethics (fields: education, culture, science), adopted June 2025.
- **Roundtables / Dialogue Circles**, e.g., the 2025 Arab Dialogue Roundtable in Cairo, culminating in a *Final Statement*.
- **AI Initiative by the LAS SG adopted in Baghdad 2025**

7. Dependencies

What the region needs / depends upon for the Working Group and related frameworks to work well:

- Commitment from national governments to adopt and implement policies aligned with the common strategy.
- Institutional capacity: Ministries, regulators, oversight bodies, experts in AI ethics, policy, law.
- Technical infrastructure: data systems, secure infrastructure, computational capacity, connectivity.
- Financial and human resources: funding, trained personnel, educational and research capacity.
- Cultural and social alignment: respect for local norms, languages; ensuring inclusivity and trust.
- Cooperation among states: harmonizing laws, standards, certification, shared platforms.

8. Connection to Other Risk / Ethical Management Initiatives

How these Arab regional efforts link with global/regional frameworks:

- The region participates in UNESCO consultations (e.g., on UNESCO Recommendation on Ethics of AI) and multistakeholder discussions.
- Cooperation with UNDP (e.g., partnership for “Digital for Sustainable Development” in Arab region).
- ALECSO’s Ethics Charter aligns with global ethics norms (values like human rights, fairness, etc.) but adapted to Arab education / culture / science context.
- MoUs with international organizations for cooperation, policy design (e.g., ICESCO, ArabNCI, etc.) reflect alignment.

9. Global / International Adoption / Implementation

The AI Arab Strategy was approved by the Arab ICT Council of Ministers.

The Secretary General Initiative on AI was approved by the Arab Leaders' Summit in 2025.

- Some deliverables are adopted: ALECSO's Charter, ongoing dialogues, projects launched by AICTO, etc. These represent initial adoption steps.
- National uptake: varying. Some Arab countries have strong national AI / ICT strategies and are incorporating ethical guidelines, regulatory frameworks, etc. Others are less advanced.
- Implementation is partial: while the strategy and charters exist, consistent enforcement, oversight, impact assessments, standardization across all states have not yet been fully realized.
- Global visibility: the Arab region's working group and initiatives are increasingly recognized in global AI governance discussions (OECD, UNESCO, etc.), especially given events like the Arab Forum on AI.
- **There is an ongoing dialogue about the mechanisms for AI governance triggered by both the strategy and the newly adopted SG Initiative.**

Islamic Organization in AI

1. Issuing Organization / Year of Release and Updates

- The Islamic world now has a **strategic & ethical framework** via the **Riyadh Charter** and **Tehran Declaration** that provide direction for AI governance in Islamic countries, aligned with Islamic values.
- So yes, there *is* an emerging framework for managing AI among Islamic organizations: it aims at cooperation, ethical guidelines, strategic vision, talent development, infrastructure, governance.
- However, **it is not yet a binding legal framework** in the sense of enforceable treaty or regulation that all member states are required to implement fully with oversight, audits, standardized impact assessment, or enforcement mechanisms.
- Much of it remains **voluntary commitments**, declarations, capacity building, research, strategy alignment. Implementation will depend heavily on individual member states adopting laws, implementing policies, oversight, etc.
- **Key Declarations / Documents:**
 - Riyadh Charter for Artificial Intelligence in the Islamic World — unanimously approved by 53 member states of ICESCO, during its 45th Executive Council session, announced during Global AI Summit in September 2024.
 - Tehran Declaration adopted by OIC15 Dialogue Platform's Second Ministerial Meeting in Tehran, May 2025, focused on "Trustworthy and Ethical Artificial Intelligence for Sustainable Development".

2. Main Objectives

From the texts of the Riyadh Charter, Tehran Declaration, and other public communications:

- Establish a **common ethical and strategic framework** for AI across Islamic countries, aligned with Islamic values.
- Promote AI for sustainable development: including in education, health, infrastructure, research, water/food security, climate change.
- Foster cooperation among member states in education, research, technology transfer, infrastructure.
- Develop “Already ecosystems” (talent, governance, best practices sharing) and publicprivate partnerships.
- Ensure “trustworthy and ethical AI” — emphasizing ethics, responsible use.

3. Legal / Regulatory Approach (Mandatory vs. Voluntary)

- So far, the approach is **largely voluntary / nonbinding**. The Riyadh Charter and Tehran Declaration are declarations or charters that express commitment, rather than enforceable treaties.
- There is no public evidence (so far) of a binding regulation across all OIC / ICESCO member states emanating from these documents.
- Member states are committing to governance, cooperation, ethical guidelines, but implementation is up to national governments.

4. Core Principles / Values / Ethical Principles

From the Riyadh Charter, Tehran Declaration:

- Alignment with **Islamic values** (e.g., ethics, values, justice, trust, shared moral perspective).
- Responsible, trustworthy AI; ethics in research; safeguarding human dignity; sustainable development.
- Justice, fairness, cooperation, knowledge sharing, talent development.
- Some scholarly works incorporate objectives of Sharia: protection of life, intellect, wealth, faith, progeny as pillars for AI ethics.
- Values like accountability, transparency, human oversight appear in academic discussions.

5. Scope

- **Lifecycle / Stages:** The documents speak generally about education, research, infrastructure, governance, and cooperation.
- **Sectors:** Education, research, science, infrastructure, as well as sustainable development sectors (health, climate, water/food security) are mentioned.
- **Stakeholders:** Member states' governments, research institutions, cultural/educational bodies (e.g., ICESCO), experts; some mention of public/private partnerships.
- **Geographic Coverage:** Member states of OIC/ ICESCO/ ISESCO (53 Islamic countries) participate.

6. Accompanying Documents / Guidelines / Tools / Projects

- **Riyadh Charter** — a shared ethical & strategic framework approved by many Islamic countries in March 2025.
- **Tehran Declaration** by the OIC15 Dialogue Platform (May 2025) focusing on AI cooperation, governance, for sustainable development etc.

7. Dependencies

- Member states must have sufficient institutional capacity (legislation, oversight, ethics committees, regulatory bodies).
- Technical and human capacity: scholars, AI experts, infrastructure.
- Harmonizing diverse Islamic legal, ethical traditions and differences between member states in readiness.
- Funding, infrastructure, research ecosystems.
- Trust and alignment with global standards while maintaining Islamic ethical identities.

8. Connection to Other Risk & Ethical Management Initiatives

- The Riyadh Charter and Tehran Declaration align with global norms of AI ethics (trustworthiness, transparency, sustainability) and with regional and global sustainable development goals.
- Some of these initiatives build on or mirror what is happening in other regions (Arab, global) regarding ethics, responsible AI, cooperative frameworks.

9. Global / International Adoption / Implementation

- The Riyadh Charter was approved by 53 Islamic countries — that shows large-scale adoption of that document in principle.
- The Tehran Declaration similarly got unanimous adoption by OIC15 Dialogue Platform members regarding cooperation etc.

The EU and CoE on governing AI

1. Issuing Organization / Country / Year of Release and Updates

- EU — AI Act: The main EU regulatory framework for AI is the EU Artificial Intelligence Act (“AI Act”). The Council of the European Union finalized it on 21 May 2024.
- CoE — Framework Convention on AI & HUDERIA: The Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law was adopted by the Council of Europe’s Committee of Ministers on 17 May 2024 and opened for signature on 5 September 2024.
- In addition, the CoE developed HUDERIA — a methodology for risk and impact assessment of AI systems from the point of view of human rights, democracy, and the rule of law. The Committee on Artificial Intelligence (CAI) of the Council of Europe adopted the HUDERIA Methodology in November 2024.
- HUDERIA is currently non-binding guidance: CoE member states (Parties to the Convention) may use or adapt it to implement their obligations under the Convention.

2. Main Objectives

- EU AI Act: The objective is to regulate AI systems placed on the EU market so that they are safe, trustworthy, and respect fundamental rights, while promoting innovation and providing a harmonized legal framework across all EU member states.
- CoE Convention + HUDERIA: The Convention aims to ensure that AI systems — at all stages (design, development, deployment, use) — are consistent with human rights, democracy, and the rule of law. HUDERIA provides a structured, humanrights-centered methodology for assessing and mitigating risks and impacts of AI systems on these values.
- The combination is intended to fill legal and ethical gaps arising from rapid AI development, and to offer a normative, rights-based governance framework for AI — compatible with regulatory enforcement (via EU law) and softlaw/advisory practice (via HUDERIA).

3. Legal and Regulatory Approach (Mandatory vs. Voluntary)

- EU AI Act: A binding regulation for EU Member States. It imposes mandatory obligations for AI systems, especially those considered “high-risk,” and bans certain unacceptable practices.
- CoE HUDERIA (via Convention): The Convention itself is a legally binding international treaty for signatories. However, HUDERIA — the Methodology for risk/impact assessment — is a nonlegally binding guidance document. Parties can choose to use or adapt HUDERIA; it does not, by itself, create new binding obligations.

4. Core Principles (Values + Ethical Principles)

With HUDERIA included, the core principles and components guiding AI governance under EU + CoE become more explicit:

- AI systems should respect human rights, democracy and the rule of law throughout their lifecycle.
- Riskbased, contextaware assessment of AI systems: HUDERIA's structure emphasises carefully analysing social, political and technical context before deployment.
- Transparency, accountability, and mitigation: HUDERIA requires identification of potential harms, evaluation (impact assessment), and mitigation plans — including remedies and safeguards when rights are at risk.
- Iterative review: AI systems should be reevaluated over their lifecycle; mitigation measures should adapt to changes in context or technology.
- Flexible, multistakeholder applicability: HUDERIA can be used by public authorities, private developers, civil society — acknowledging that responsible AI governance requires involvement beyond state actors.

5. Scope

- **EU AI Act:** Covers all AI systems placed on or used in the EU, by public or private actors. It aims to govern the entire AI lifecycle (design, development, deployment, use).
- **CoE Convention + HUDERIA:** Applies to AI systems in jurisdictions that adopt the Convention. HUDERIA's scope is broad — any AI system whose deployment could affect human rights, democracy or the rule of law. Its methodology is intended to be adaptable to many domains and contexts.

6. Accompanying Documents / Guidelines / Tools / Projects

- **HUDERIA Methodology:** Detailed guidance, providing structured steps for risk & impact assessments, including context-based analysis, risk identification, impact assessment, mitigation planning, and ongoing evaluation.
- The CoE has committed to publishing the HUDERIA Model in 2025 — a supporting library of resources, tools, and scalable recommendations to help implement the HUDERIA methodology.
- For the EU: the official legislative texts of the AI Act, along with its accompanying risk classification and compliance guidelines (publicly available via EU institutions).

7. Dependencies

Effective implementation of AI governance under this combined EU + CoE approach depends on:

- Member states' willingness to ratify the CoE Convention, and to adopt/adapt HUDERIA in national contexts.
- Institutional capacity: regulatory agencies, humanrights bodies, auditors, technical experts for risk assessment and oversight.
- Engagement of stakeholders: public authorities, private sector developers, civil society organisations, and independent experts.
- Alignment with other laws and standards (e.g. data protection, nondiscrimination laws), and willingness to integrate risk/impact assessments into procurement, deployment, and audit processes.
- Continuous monitoring and iterative reassessment, to respond to evolving AI technologies and societal contexts — a core requirement of HUDERIA.

8. Connection to Other Risk & Ethical Management Initiatives

Including HUDERIA helps bridge regulatory and nonregulatory AI governance efforts:

- HUDERIA complements the binding EU AI Act by offering a humanrightscentered, rightsbased assessment methodology, bridging technical risk management with social, legal and ethical considerations.
- By designing a methodology tailored to rights, democracy and rule of law — but flexible and nonbinding — HUDERIA encourages **voluntary compliance and best practices**, which can align with other international standards (e.g. data protection, ethical AI frameworks).
- The dual approach (binding regulation + softlaw methodology) helps the EU and CoE balance **innovation, regulation, and human rights protection**.

9. Global / International Adoption / Implementation

- The CoE Convention (and HUDERIA) is open to accession by any state, offering a path for countries beyond Europe to adopt **rightscentered AI governance**.
- As the EU is a signatory to the Convention, the combined framework becomes a **model — both legally enforceable and ethically grounded** — that could influence global AI regulation and standards

Appendix G: Detailed Profiles of Sectoral Regulations

Healthcare

***Document Title*:** Ethics and Governance of Artificial Intelligence for Health

Issuing Authority: World Health Organization (WHO)

Country/Org: Global Organization

Issuing Date: June 2021

URL: <https://www.who.int/publications/i/item/9789240029200>

Document Type: Administrative Rules (Global Guidance & Principles)

Summary: Provides a global normative framework for the responsible design, development, and deployment of AI for health. It establishes six core principles: protect autonomy; promote human well-being, safety, and the public interest; ensure transparency, explainability, and intelligibility; foster responsibility and accountability; ensure inclusiveness and equity; and promote AI that is responsive and sustainable. It emphasizes ethical and human rights standards, data diversity, and the impact on healthcare workers.

***Document Title*:** FDA Artificial Intelligence/Machine Learning (AI/ML)-Enabled Medical Devices: Action Plan

Issuing Authority: U.S. Food and Drug Administration (FDA)

Country/Org: United States

Issuing Date: January 2021

URL: <https://www.fda.gov/media/145022/download>

Document Type: Administrative Rules (Guidance and Policy Framework)

Summary: Outlines the FDA's evolving approach to AI/ML-based Software as a Medical Device (SaMD), building on existing frameworks. It champions a total product lifecycle (TPLC) approach, good machine learning practices (GMLP), and the development of a "Predetermined Change Control Plan" for safe and effective iterative model updates.

***Document Title*:** Content of Premarket Submissions for Device Software Functions Including Machine Learning (ML) - Guided Industry

Issuing Authority: U.S. Food and Drug Administration (FDA)

Country/Org: United States

Issuing Date: September 2023 (Final Guidance)

URL: <https://www.fda.gov/media/167973/download>

Document Type: Administrative Rules (Final Guidance)

Summary: The primary FDA guidance mandating rigorous documentation of the entire ML lifecycle (data management, training, evaluation) and a "Predetermined Change Control Plan" (PCCP) to ensure ongoing safety and effectiveness of AI/ML in medical devices.

***Document Title*:** Software and AI as a Medical Device Change Program - Roadmap

Issuing Authority: Medicines and Healthcare products Regulatory Agency (MHRA)

Country/Org: United Kingdom

Issuing Date: Updated Regularly

URL: <https://www.gov.uk/government/publications/software-and-ai-as-a-medical-device-change-programme/software-and-ai-as-a-medical-device-change-programme-roadmap>

Document Type: Administrative Rules (Guidance and Policy Framework)

Summary: The UK MHRA's roadmap clarifies the regulatory pathway for AI and software used in medical devices. It addresses specific challenges like transparency and interpretability, aiming to adapt the UK's regulatory framework to be more agile and supportive of innovation while ensuring patient safety.

***Document Title*:** A Guide to Good Practice for Digital and Data-Driven Health Technologies

Issuing Authority: National Health Service (NHS) England

Country/Org: United Kingdom

Issuing Date: Regularly Updated

URL: <https://www.nhsx.nhs.uk/ai-lab/ai-lab-programmes/regulation/guide-to-good-practice/>

Document Type: Industry Technical Standard / Procurement Standard

Summary: The de facto standard for AI vendors in the UK's NHS. Outlines principles for clinical safety, cybersecurity, data protection, and algorithmic fairness, making compliance essential for market access.

***Document Title*:** Guidelines for the Review and Approval of Artificial Intelligence (AI) Medical Devices

Issuing Authority: Ministry of Food and Drug Safety (MFDS)

Country/Org: South Korea

Issuing Date: Ongoing Updates

URL (Example): https://www.mfds.go.kr/eng/brd/m_65/view.do?seq=12 (MFDS English Portal)

Document Type: Administrative Rules (Binding Regulation & Guidance)

Summary: South Korea's MFDS has established clear classification guidelines for AI-powered medical devices. It mandates rigorous clinical trials, especially for AI-based diagnostic tools, to validate performance, accuracy, and safety before market approval, reflecting a highly cautious and evidence-based approach.

***Document Title*:** Guiding Principles for the Technical Review of Artificial Intelligence Medical Devices (Deep Learning) and related updates.

Issuing Authority: National Medical Products Administration (NMPA)

Country/Org: China

Issuing Date: Initial 2019, with ongoing updates

URL (Example in Chinese): <http://www.nmpa.gov.cn/WS04/CL2138/375583.html>

Document Type: Administrative Rules (Binding Regulation & Guidance)

Summary: China's NMPA has issued specific guidelines for deep learning applications in medical devices. Its regulatory approach has evolved from a pre-market focus towards a lifecycle-based continuous oversight model for AI medical software, emphasizing real-world performance monitoring and post-market surveillance.

***Document Title*:** Draft Guidelines for Responsible AI Development and Use in Healthcare

Issuing Authority: Health Sciences Authority (HSA) and Ministry of Health (MOH)

Country/Org: Singapore

Issuing Date: 2023 (Draft)

URL: [Typically published on HSA or MOH websites for consultation]

Document Type: Administrative Rules (Draft Guidance)

Summary: These draft guidelines focus on the safe development and implementation of AI in healthcare. Key pillars include ensuring model explainability, using high-quality and representative training data, and implementing comprehensive risk controls throughout the AI lifecycle, positioning Singapore as a leader in pragmatic AI governance.

***Document Title*:** ISO/IEC 81001-5-1:2021 Health software and health IT systems safety, effectiveness, and security.

Issuing Authority: ISO/IEC

Country/Org: Global Organization

Issuing Date: 2021

URL: <https://www.iso.org/standard/80670.html>

Document Type: Industry Technical Standard

Summary: Provides a critical risk-management framework for the security, safety, and effectiveness of health software, including AI components. Essential for securing training data and ensuring model robustness against adversarial attacks in medical systems.

***Document Title*:** The EU Artificial Intelligence Act

Issuing Authority: European Parliament and Council

Country/Org: European Union

Issuing Date: March 2024

URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>

Document Type: Administrative Rules (Binding Regulation)

Summary: Classifies AI used in diagnostics, triage, and therapeutic treatment as high-risk. This mandates conformity assessment with strict ex-ante requirements for risk management, high-quality datasets, technical documentation, and human oversight before these devices can be placed on the EU market.

This integrated list provides a comprehensive global overview, ranging from high-level ethical principles (WHO) to specific national implementation guidelines (MFDS, NMPA, HSA), all underpinned by regional binding law (EU AI Act) and international technical standards (ISO).

Education

***Document Title*:** AI and Education: Guidance for Policymakers.

Issuing Authority: UNESCO

Country/Org: Global Organization

Issuing Date: 2021

URL: <https://unesdoc.unesco.org/ark:/48223/pf0000376709>

Document Type: Administrative Rules (Policy Guidance)

Summary: A foundational human-centric framework for integrating AI into education. It emphasizes inclusion, equity, and the protection of student data. It calls for banning AI systems that undermine human dignity and ensuring human oversight in educational decision-making.

***Document Title*:** Digital Education Action Plan (2021-2027)

Issuing Authority: European Commission

Country/Org: European Union

Issuing Date: September 2020

URL: <https://education.ec.europa.eu/focus-topics/digital-education/action-plan>

Document Type: Administrative Rules (Strategic Policy Framework)

Summary: This strategic initiative explicitly calls for promoting AI and data literacy among students and citizens. It aims to foster a deeper understanding of AI's opportunities and risks, equipping individuals with the skills to engage with AI critically and responsibly.

***Document Title*:** P2863 - Recommended Practice for Organizational Governance of Artificial Intelligence in Education

Issuing Authority: IEEE

Country/Org: Global Organization

Issuing Date: Under Development

URL: <https://standards.ieee.org/ieee/2863/10775/>

Document Type: Industry Technical Standard (Draft)

Summary: Forthcoming standard providing a technical and operational framework for the responsible deployment of AI in educational institutions, covering governance, ethical risk assessment, and data stewardship.

***Document Title*:** The EU Artificial Intelligence Act

Issuing Authority: European Parliament and Council

Country/Org: European Union

Issuing Date: March 2024

URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>

Document Type: Administrative Rules (Binding Regulation)

Summary: Directly regulates the use of AI systems in education by classifying AI used for determining access to educational institutions or for scoring exams as high-risk. This mandates strict requirements for transparency, data governance, and human oversight to prevent bias and ensure fairness.

This integrated view now clearly distinguishes between:

Regulatory Frameworks governing the deployment and use of AI tools within educational settings (e.g., EU AI Act, UNESCO Guidance).

National Capacity-Building Strategies focused on teaching about AI and building a skilled workforce for the future (e.g., plans from the UK, China, Singapore, South Korea, and India).

This distinction is crucial for policymakers and educators to navigate their respective responsibilities effectively.

Fintech

***Document Title*:** AI in Finance

Issuing Authority: Organization for Economic Co-operation and Development (OECD)

Country/Org: Global Organization

Issuing Date: Ongoing (e.g., 2021 Report “AI in Finance”)

URL: <https://www.oecd.org/finance/ai-in-finance.htm>

Document Type: Administrative Rules (Policy Analysis & Guidance)

Summary: The OECD publishes extensive analysis and policy papers on AI in finance, comparing regulatory approaches across its member states. Its work helps shape international consensus on principles for responsible AI, focusing on financial stability, consumer protection, and market integrity.

***Document Title*:** Principles on Artificial Intelligence

Issuing Authority: OECD

Country/Org: Global Organization

Issuing Date: May 2019

URL: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>

Document Type: Administrative Rules (International Agreement)

Summary: Although horizontal, the OECD AI Principles are adopted by many countries and provide the foundational ethical framework (inclusive growth, human rights, transparency, robustness) that underpins many national fintech AI guidelines.

National & Regional Regulations

***Document Title*:** Artificial Intelligence and Machine Learning (DP22/5)

Issuing Authority: Bank of England / Prudential Regulation Authority (PRA) & Financial Conduct Authority (FCA)

Country/Org: United Kingdom

Issuing Date: October 2022

URL: <https://www.bankofengland.co.uk/prudential-regulation/publication/2022/october/artificial-intelligence-and-machine-learning-discussion-paper>

Document Type: Administrative Rules (Consultation & Forthcoming Guidance)

Summary: The UK regulators have conducted extensive surveys and issued this discussion paper outlining expectations for the safe use of AI/ML. Their focus is on robust model risk management, explainability, governance, and consumer protection, signaling the future of binding expectations.

***Document Title*:** Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector

Issuing Authority: Monetary Authority of Singapore (MAS)

Country/Org: Singapore

Issuing Date: November 2018

URL: <https://www.mas.gov.sg/regulation/guidelines/feat-principles>

Document Type: Administrative Rules (Sector-Specific Guidance)

Summary: A pioneering sector-specific framework. The FEAT principles provide detailed guidance on ensuring fairness (addressing bias), ethicality, accountability (clear responsibility), and transparency (communications and explainability) in AI-driven financial services, supported by the Veritas initiative for industry implementation.

***Document Title*:** Joint Statement on Machine Learning in Credit Underwriting

Issuing Authority: OCC, Federal Reserve, FDIC, NCUA, Consumer Financial Protection Bureau (CFPB)

Country/Org: United States

Issuing Date: 2021

URL: <https://www.federalreserve.gov/supervisionreg/spleters/2021-joint-statement-on-machine-learning-in-credit-underwriting.htm>

Document Type: Administrative Rules (Interagency Guidance)

Summary: The CFPB and other US regulators explicitly apply existing laws like the Equal Credit Opportunity Act (ECOA) to AI. They mandate that models must be explainable enough to provide accurate adverse action notices and must not result in illegal discrimination, enforcing fairness through consumer protection law.

***Document Title*:** Artificial Intelligence and Machine Learning in Financial Services

Issuing Authority: Central Bank of the UAE (CBUAE), Dubai Financial Services Authority (DFSA), Financial Services Regulatory Authority (FSRA) of ADGM

Country/Org: United Arab Emirates

Issuing Date: 2021

URL (Example - DFSA): <https://www.dfsa.ae/News-Articles/2021/UAE-Financial-Regulatory-Authorities-issue-Joint-Guidelines-on>

Document Type: Administrative Rules (Joint Guidance)

Summary: The UAE's key financial regulators issued joint guidelines providing a unified framework for financial institutions. The guidelines focus on sound governance structures, clear accountability for AI outcomes, and ensuring transparency in AI-driven customer interactions and decisions.

***Document Title*:** Artificial intelligence in financial sector activities – FIN-FSA's observations and recommendations.

Issuing Authority: Financial Supervisory Authority of Finland (FIN-FSA)

Country/Org: Finland (European Union)

Issuing Date: November 2023

URL: <https://www.fin-fsa.fi/en/publications-and-press-releases/news/2023/artificial-intelligence-in-financial-sector-activities--fin-fsa-s-observations-and-recommendations/>

Document Type: Administrative Rules (Supervisory Guidance)

Summary: Provides practical insights for financial institutions on preparing for and complying with the EU AI Act. It clarifies how the high-risk classification for AI in credit scoring and risk management will be interpreted and enforced, emphasizing the need for robust governance, data quality, and human oversight.

***Document Title*:** Artificial Intelligence in the Japanese Financial Sector

Issuing Authority: Japan's Financial Services Agency (FSA)

Country/Org: Japan

Issuing Date: August 2023 (Draft Principles)

URL: <https://www.fsa.go.jp/en/regulated/ai/20230825/01.pdf>

Document Type: Administrative Rules (Draft Principles)

Summary: Comprehensive principles for AI in finance, covering governance, risk management, fairness (including bias mitigation), transparency, and security in applications like credit scoring and algorithmic trading.

***Document Title*:** The EU Artificial Intelligence Act

Issuing Authority: European Parliament and Council

Country/Org: European Union

Issuing Date: March 2024

URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>

Document Type: Administrative Rules (Binding Regulation)

Summary: Classifies AI systems used for creditworthiness assessment and risk pricing for life and health insurance as high-risk. This mandates conformity assessment with strict requirements for risk management, data governance, technical documentation, and human oversight before deployment.

This provides a comprehensive roadmap for any financial institution navigating global AI compliance.

Energy

***Document Title*:** Data-driven and Artificial Intelligence (AI) Tools in the Energy Sector: Key Guidelines

Issuing Authority: International Energy Agency (IEA)

Country/Org: Global Organization

Issuing Date: 2023

URL: <https://www.iea.org/reports/data-driven-and-artificial-intelligence-ai-tools-in-the-energy-sector-key-guidelines>

Document Type: Administrative Rules (Policy Guidance)

Summary: This report provides a sector-specific analysis of AI applications in energy (e.g., grid optimization, predictive maintenance) and outlines key policy guidelines. It emphasizes the need for data accessibility, model interoperability, cybersecurity for critical infrastructure, and workforce training.

***Document Title*:** ISO/IEC 27001:2022 Information security, cybersecurity, and privacy protection.

Issuing Authority: ISO/IEC

Country/Org: Global Organization

Issuing Date: 2022

URL: <https://www.iso.org/standard/27001>

Document Type: Industry Technical Standard

Summary: As energy systems become more digitalized and reliant on AI, cybersecurity is paramount. Certifying AI systems and their supporting infrastructure to this standard is critical for protecting operational technology (OT) and preventing disruptions to critical energy infrastructure from cyber-attacks.

National & Regional Regulations

***Document Title*:** Ethical AI use in the energy sector.

Issuing Authority: Office of Gas and Electricity Markets (Ofgem)

Country/Org: United Kingdom

Issuing Date: 2023

URL: <https://www.ofgem.gov.uk/publications/ethical-ai-use-energy-sector>

Document Type: Administrative Rules (Sector-Specific Guidance)

Summary: This guidance promotes good practice for the safe, secure, fair, and environmentally sustainable deployment of AI by energy companies. It directly addresses sector-specific concerns such as ensuring AI does not disrupt grid stability, protects consumer data, and contributes to decarbonization goals.

***Document Title*:** Artificial Intelligence (AI) Usage Guidelines

Issuing Authority: U.S. Department of Energy (DOE)

Country/Org: United States

Issuing Date: 2023

URL: <https://www.energy.gov/diversity/articles/department-energy-releases-artificial-intelligence-ai-usage-guidelines>

Document Type: Administrative Rules (Internal & Extramural Guidance)

Summary: These guidelines govern the development and deployment of AI within the DOE's vast operations, which include managing the national nuclear security complex and critical energy infrastructure. The focus is on responsible AI use, with principles covering safety, security, fairness, and accountability in high-stakes environments.

***Document Title*:** Energy Efficiency Act (Energieeffizienzgesetz - EnEg)

Issuing Authority: German Federal Government

Country/Org: Germany

Issuing Date: 2023 (Passed)

URL: <https://www.bmwk.de/Redaktion/DE/Gesetze/Energie/eneffg.html>

Document Type: Administrative Rules (Binding National Legislation)

Summary: This act includes specific regulations for the energy consumption and efficiency of data centers. This is an indirect but critical form of AI governance, as it imposes strict requirements on the power usage and waste heat utilization of the large data centers that underpin energy-intensive AI model training and inference, pushing the industry toward greater sustainability.

***Document Title*:** The EU Artificial Intelligence Act

Issuing Authority: European Parliament and Council

Country/Org: European Union

Issuing Date: March 2024

URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>

Document Type: Administrative Rules (Binding Regulation)

Summary: Classifies AI systems intended for use as safety components in the management and operation of critical infrastructure (including electricity and gas) as high-risk. This means AI used for grid management, load balancing, or pipeline control will be subject to strict ex-ante requirements for risk management, data governance, and robustness to ensure they do not endanger public safety or disrupt essential services.

This integrated summary now captures the multi-faceted approach to AI governance in the energy sector:

Critical Infrastructure Protection: Through binding law (EU AI Act) and cybersecurity standards (ISO 27001).

Ethical and Sustainable Deployment: Through sector-specific guidance (UK Ofgem) and internal governance (US DOE).

Environmental Impact Mitigation: Through legislation targeting the resource footprint of the underlying AI infrastructure itself (Germany's Energy Efficiency Act).

Transportation

***Document Title*:** UN Regulation No. 157 - Uniform provisions concerning the approval of vehicles with regard to Automated Lane Keeping Systems

Issuing Authority: UNECE World Forum for Harmonization of Vehicle Regulations (WP.29)

Country/Org: Global Organization (58 contracting parties including EU, Japan, UK)

Issuing Date: March 2021

URL: <https://unece.org/transport/documents/2021/03/standards/un-regulation-no-157-automated-lane-keeping-systems>

Document Type: Administrative Rules (Binding International Regulation)

Summary: The first binding international regulation for Level 3 automated driving systems (Automated Lane Keeping Systems - ALKS). It sets strict, uniform technical requirements for safety-performance, cybersecurity, fail-safe operation, and Data Storage Systems for Automated Driving (DSSAD) - the "black box" for automated vehicles.

***Document Title*:** SAE J202104_3016: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles

Issuing Authority: SAE International

Country/Org: Global Organization

Issuing Date: April 2021

URL: https://www.sae.org/standards/content/j3016_202104/

Document Type: Industry Technical Standard

Summary: The foundational global standard that defines the six levels of driving automation (0-5), from no automation to full automation. It provides the common language used by regulators, manufacturers, and developers worldwide to ensure clarity and consistency.

National & Regional Regulations

***Document Title*:** AI Assurance for Transportation

Issuing Authority: U.S. Department of Transportation (DOT)

Country/Org: United States

Issuing Date: 2024

URL: <https://www.transportation.gov/airconsumer/AI-Assurance-Transportation>

Document Type: Administrative Rules (Policy Framework & Guidance)

Summary: This white paper outlines a flexible, “assurance-based” framework for the safe and secure integration of AI into safety-critical transportation systems (aviation, automotive, rail, etc.). It emphasizes an agency-led, context-specific approach rather than a one-size-fits-all rule, focusing on achieving safety outcomes through rigorous testing, validation, and continuous monitoring.

***Document Title*:** Management Standards for Road Testing of Intelligent Connected Vehicles and related regulations.

Issuing Authority: Ministry of Industry and Information Technology (MIIT), Ministry of Transport, et al.

Country/Org: China

Issuing Date: Ongoing since 2018

URL (Example): http://www.gov.cn/zhengce/2021-07/30/content_5628546.htm (Policy on industrial development)

Document Type: Administrative Rules (Binding National Regulations)

Summary: China has enacted a comprehensive set of legally binding rules specifically for the management and safety of autonomous vehicles. These cover road testing, licensing, data security, and accident liability. They are part of a broader national strategy to dominate the smart transportation sector, with specific rules also targeting AI in public transport infrastructure.

***Document Title*:** The EU Artificial Intelligence Act

Issuing Authority: European Parliament and Council

Country/Org: European Union

Issuing Date: March 2024

URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>

Document Type: Administrative Rules (Binding Regulation)

Summary: Classifies AI systems used in aviation safety and as safety components of road vehicles and railways as high-risk. This mandates that AI for traffic control, advanced driver assistance systems (ADAS), and other safety-critical applications undergo strict conformity assessment for risk management, data quality, and robustness before being placed on the market.

Context: Various National Road Safety Bodies

Summary: Beyond the major frameworks listed, numerous countries have their own national bodies (e.g., Germany’s KBA, Japan’s MLIT) developing specific rules for the testing, deployment, and liability of autonomous vehicles. These often build upon the UNECE WP.29 framework but add national requirements, creating a complex global patchwork that manufacturers must navigate.

This integrated summary now captures the layered regulatory environment for AI in

transportation:

International Harmonization: Through binding UNECE regulations and voluntary SAE standards to enable global market access.

Regional Risk-Based Regulation: The EU AI Act's ex-ante approach for high-risk AI systems in vehicles and infrastructure.

National Assurance Frameworks: The U.S. DOT's context-specific, outcome-oriented approach to safety assurance.

National Strategic Regulation: China's comprehensive, prescriptive legal framework aimed at industry leadership.

A Global Patchwork: The ongoing development of specific, often divergent, national rules for AV testing and liability.

Manufacturing

***Document Title*:** ISO/IEC 42001:2023 Information technology — Artificial intelligence — Management system.

Issuing Authority: International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC)

Country/Org: Global Organization

Issuing Date: 2023

URL: <https://www.iso.org/standard/81230.html>

Document Type: Industry Technical Standard

Summary: This is the world's first AI-specific management system standard. It provides a framework for establishing, implementing, and maintaining an Artificial Intelligence Management System (AIMS). For manufacturers, it is a critical tool for systematically managing AI risks and opportunities across operations like predictive maintenance, robotics, and supply chain optimization, ensuring responsible and transparent AI use.

***Document Title*:** ISO/IEC 23053:2022 Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)

Issuing Authority: ISO/IEC JTC 1

Country/Org: Global Organization

Issuing Date: 2022

URL: <https://www.iso.org/standard/74438.html>

Document Type: Industry Technical Standard

Summary: This standard establishes a generic framework for AI systems using machine learning, which is universally applicable in smart manufacturing and industrial IoT. It describes the ML lifecycle and functional workflow, providing a common structure for integrating AI into production systems and robotics, ensuring interoperability and systematic development.

Context: Industry & Consultancy Frameworks (e.g., IBM's AI Ethics Framework, PwC's Responsible AI Toolkit)

Issuing Authority: Industry Bodies & Consultancies

Country/Org: Global

Document Type: Industry Technical Standards & Best Practices

Summary: While not legally binding, these frameworks are highly influential. They provide mature, detailed guidelines that align with standards like ISO 42001. They emphasize data integrity and transparency for quality control and predictive maintenance, human oversight in automated processes, and comprehensive risk assessment. A key focus is ensuring AI systems in manufacturing comply with overarching regulations like the GDPR for employee and operational data.

National & Regional Regulations

***Document Title*:** The EU Artificial Intelligence Act

Issuing Authority: European Parliament and Council

Country/Org: European Union

Issuing Date: March 2024

URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>

Document Type: Administrative Rules (Binding Regulation)

Summary: While horizontal, the AI Act has profound implications for manufacturing. It classifies AI systems used in safety components of machinery (e.g., AI-driven industrial robots, quality control systems) as high-risk. This subjects them to strict ex-ante requirements for risk management, data governance, technical documentation, and human oversight before they can be placed on the EU market.

***Document Title*:** Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

Issuing Authority: The White House

Country/Org: United States

Issuing Date: October 2023

URL: <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/>

Document Type: Administrative Rules (Executive Order)

Summary: This EO directs agencies, including the Department of Commerce and NIST, to develop and use consensus standards for AI. For manufacturing, this means that frameworks like the NIST AI RMF and future sector-specific guidelines will become increasingly important for federal procurement and setting de facto industry standards for safe and trustworthy industrial AI.

This integrated summary highlights the unique regulatory posture for manufacturing AI: Standards-Led Governance: The primary drivers are international technical standards (ISO 42001, 23053) and industry best practices, which provide actionable blueprints for implementation.

Indirect Regulation via Product Safety: Binding law often enters through product safety and machinery directives (as seen in the EU AI Act), regulating AI as a component of physical equipment.

Horizontal Law Application: General data protection (GDPR), cybersecurity, and liability laws provide the mandatory legal floor, while industry standards build upon it to address sector-specific challenges like supply chain resilience and human-robot collaboration.

Agriculture

***Document Title*:** OECD-FAO Guidance for Responsible Agricultural Supply Chains: A focus on due diligence for the use of digital technology.

Issuing Authority: Organization for Economic Co-operation and Development (OECD) & UN Food and Agriculture Organization (FAO)

Country/Org: Global Organization

Issuing Date: 2023

URL: <https://www.oecd.org/en/topics/agriculture-and-food-systems/oecd-fao-guidance-for-responsible-agricultural-supply-chains.html>

Document Type: Administrative Rules (International Guidance)

Summary: This guidance integrates AI governance into the broader context of sustainable agriculture. It advises companies on conducting due diligence when deploying digital technologies, including AI, in their supply chains. It addresses sector-specific risks such as the impact of automation on smallholder farmers, data ownership of farm data, and ensuring AI-driven recommendations for pesticide or water use are sustainable and equitable.

Context: OECD Reports on AI in the Agri-Food Sector

Issuing Authority: Organization for Economic Co-operation and Development (OECD)

Country/Org: Global Organization

Summary: The OECD has published extensive analysis on AI in agriculture, providing recommendations on user-centric (farmer-focused) data governance models. Their work emphasizes promoting equity, transparency, and data security to manage critical risks like algorithmic bias that could disadvantage small-scale farms in favor of large-scale agribusiness.

National & Regional Regulations

***Document Title*:** MahaAgri-AI Policy 2025–2029

Issuing Authority: Government of Maharashtra (India)

Country/Org: India

Issuing Date: 2024 (Draft/Announced)

URL: [Typically published on the Maharashtra Department of Agriculture website]

Document Type: Administrative Rules (Sub-National Policy & Roadmap)

Summary: A pioneering example of a sub-national AI policy focused exclusively on agriculture. This roadmap outlines a comprehensive strategy for transforming the state's agricultural sector through AI. It includes specific governance frameworks for data traceability and quality, aiming to ensure that AI applications in areas like precision farming, yield prediction, and market access are reliable, equitable, and beneficial for farmers.

***Document Title*:** National Strategy for Artificial Intelligence (#AIforAll)

Issuing Authority: NITI Aayog (Government of India)

Country/Org: India

Issuing Date: June 2018

URL: <https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf>

Document Type: Administrative Rules (National Strategic Plan)

Summary: India's national strategy explicitly identifies agriculture as a priority sector for AI application. It focuses on areas such as predictive analytics for crop yields, soil health monitoring, and personalized farm advisories, setting the stage for more detailed policies like the MahaAgri-AI initiative.

***Document Title*:** The EU Artificial Intelligence Act

Issuing Authority: European Parliament and Council

Country/Org: European Union

Issuing Date: March 2024

URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>

Document Type: Administrative Rules (Binding Regulation)

Summary: The AI Act is highly relevant to agriculture as it explicitly classifies AI systems intended for use in employment and workforce management as high-risk. This directly impacts large-scale farms and agribusinesses using AI for seasonal worker management, performance evaluation, and task assignment, requiring fundamental rights impact assessments and transparency.

This integrated summary reveals the evolving layers of agricultural AI governance:

International Guidance: Framing the core challenges of equity, sustainability, and data rights (OECD/FAO).

Horizontal Regulation: Applying broad rules (like the EU AI Act) to specific agricultural use-cases, particularly in labor management.

National & Sub-National Strategy: Moving from national vision (India's strategy) to operational, on-the-ground implementation with detailed data governance frameworks (MahaAgri-AI Policy), which is where the most sector-specific rules are currently emerging.

Appendix H: Detailed Profiles of Sectoral Regulations

Definitions of the four “State Roles” that define the global governance models:

1. State as Referee

Definition: The government steps back to let the private sector lead innovation. It acts as an impartial arbiter that only intervenes “**ex-post**” (after the fact) to penalize specific harms or enforce fair play, rather than dictating how technology should be built.

Motto: “Play the game, we will blow the whistle if you foul.”

2. State as Guardian

Definition: The government acts as a protector of fundamental rights and safety. It enforces strict “**ex-ante**” (before the fact) rules and conformity assessments to prevent dangerous AI from entering the market, prioritizing public safety over speed.

Motto: “Safety first; prove it is safe before you sell it.”

3. State as Architect

Associated Model: Hybrid / Strategic (e.g., Saudi Arabia, India).

Definition: The government actively **designs and builds** the ecosystem. It does not just regulate; it funds and owns the critical infrastructure (Sovereign Clouds, National Models) and directs the market toward specific national economic goals.

Motto: “We will build the foundation and direct where the industry goes.”

4. State as Cultivator

Associated Model: Foundational / Developing (e.g., Kenya, South Africa).

The government focuses on capacity-building. Its primary role is to create the necessary conditions for AI to grow (infrastructure, data, skills) and establish ethical baselines, avoiding premature regulation that might kill the nascent industry.

Motto: “Prepare the soil (infrastructure/skills) so innovation can take root.”

