Global AI Regulatory Mapping Template

A Multijurisdiction Governance Template for Mapping AI Obligations Across the EU AI Act, NIST AI RMF, OECD Principles, ISO/IEC 42001, and Related Frameworks

AI Governance Desk
www.aigovernancedesk.com

Edition 1.0 — 2026

Copyright, Disclaimer, and Intended Use

COPYRIGHT NOTICE

DISCLAIMER

This template is provided for educational and governance-support purposes only. It does not constitute legal advice, regulatory guidance, or professional compliance assurance.

Organizations using this template are responsible for ensuring that their implementation aligns with applicable laws, regulations, and sector-specific requirements. Legal counsel or qualified compliance professionals should be consulted where necessary.

While this document reflects widely recognized frameworks, including the EU AI Act, NIST AI Risk Management Framework, OECD AI Principles, and ISO/IEC 42001, it does not guarantee compliance with any specific jurisdiction.

INTENDED USE

This template is designed to support organizations in mapping AI governance obligations across multiple frameworks and jurisdictions. It should be adapted to reflect the specific operational context, risk profile, and regulatory exposure of each organization.

The content is intended for use by governance teams, legal departments, compliance professionals, product teams, and risk management stakeholders.

Document Control and Versioning

Document ID: ______________________________

Version: ______________________________

Owner: ______________________________

Reviewer: ______________________________

Approval Date: ______________________________

Next Review Date: ______________________________

Applicable Jurisdictions:

____

____

Business Unit / Department:

____

____

Document Classification:

□ Public
□ Internal
□ Confidential
□ Restricted

Document Status:

□ Draft
□ Under Review
□ Approved
□ Archived

This document must be reviewed periodically to ensure continued alignment with applicable regulatory frameworks and organizational governance requirements.

Executive Summary

WHAT THIS IS

This Global AI Regulatory Mapping Template is designed to help organizations structure and align their AI governance obligations across multiple regulatory frameworks. It provides a practical foundation for identifying, documenting, and managing requirements from instruments such as the EU AI Act, NIST AI Risk Management Framework, OECD AI Principles, and ISO/IEC 42001.

WHY IT EXISTS

As AI governance becomes increasingly complex across jurisdictions, organizations face challenges in maintaining consistency, avoiding duplication, and demonstrating compliance. This template addresses that gap by offering a structured approach to mapping obligations, aligning controls, and supporting cross-functional governance processes.

WHO IT IS FOR

This template is intended for use by governance teams, compliance professionals, legal departments, risk managers, and product teams responsible for developing, deploying, or overseeing AI systems in regulated or multi-jurisdictional environments.

WHEN TO USE IT

It is most effective when used during system design, regulatory assessment, internal audits, vendor evaluations, and ongoing monitoring activities. The template supports both initial governance setup and continuous alignment as regulatory expectations evolve.

Key Value

- Aligns multiple frameworks in one structure
- Reduces duplication and compliance friction
- Supports audit readiness and documentation
- Enables consistent governance across jurisdictions

How to Use This Template

This template is designed to be used as a structured workflow for aligning AI governance requirements across multiple frameworks. Follow the steps below to ensure consistency, completeness, and audit readiness.

Step-by-Step Usage

1. Inventory AI Systems

Identify all AI systems within your organization, including internally developed and third-party systems.

2. Classify Risk Levels

Assess and categorize each system based on risk exposure, regulatory impact, and operational significance.

3. Map Applicable Obligations

Align each system with relevant requirements from the EU AI Act, NIST AI RMF, OECD Principles, and other applicable frameworks.

4. Assign Evidence and Documentation

Attach supporting documentation, including risk assessments, technical records, and compliance evidence.

5. Assign Ownership and Responsibility

Define clear accountability by assigning system owners, reviewers, and governance roles.

6. Identify Gaps and Mitigation Actions

Analyze gaps between current practices and regulatory expectations, and define corrective actions.

7. Establish Review and Monitoring Cycles

Set periodic review timelines to ensure continuous compliance and alignment with evolving regulations.

Frameworks Covered in This Template

This template brings together the most influential AI governance frameworks in use today, helping organizations align their systems across different regulatory environments. Each framework plays a distinct role, whether legal, operational, or strategic.

EU AI Act (European Union)

A legally binding framework that introduces a structured, risk-based approach to regulating AI systems, especially those considered high-risk.
Role in this template: Serves as the primary legal baseline for classification, obligations, and compliance requirements.

NIST AI Risk Management Framework (AI RMF 1.0)

A widely adopted framework that helps organizations manage AI risks through practical functions such as governance, mapping, measurement, and control.
Role in this template: Translates regulatory expectations into actionable risk management processes.

OECD AI Principles

A globally recognized set of principles focused on responsible AI, emphasizing transparency, fairness, accountability, and human-centered design.
Role in this template: Provides a shared international foundation for trustworthy AI governance.

ISO/IEC 42001 (AI Management System Standard)

A formal management system standard designed to embed AI governance into organizational structures, including policies, controls, and continuous improvement mechanisms.
Role in this template: Acts as the operational backbone for maintaining governance consistency.

Supporting Frameworks:

United States Executive Order on AI (Policy Context)

A policy-driven framework shaping expectations around safety, transparency, and accountability in AI development within the U.S. landscape.
Role in this template: Reflects evolving regulatory direction and enforcement signals.

Council of Europe AI Convention (Human Rights Context)

A treaty-based framework addressing the impact of AI on human rights, democratic values, and the rule of law.
Role in this template: Reinforces rights-based governance considerations across jurisdictions.

Framework Type and Interpretation Guide

Understanding the nature of each framework is essential for correct implementation. Not all frameworks carry the same legal weight or operational role. This guide clarifies how each type should be interpreted and applied within a governance program.

Framework Classification Legend

Framework	Type	Legal Weight	Scope	Role in Template
EU AI Act	Binding Regulation	Mandatory	EU / Global Impact	Defines legal obligations and classification baseline
NIST AI RMF	Voluntary Framework	Non-binding	US / Global	Guides risk management implementation
OECD AI Principles	Principles-Based	Advisory	Global	Provides ethical and governance foundation
ISO/IEC 42001	Management Standard	Certifiable	Global	Structures governance systems and controls
US Executive Order	Policy Framework	Semi-binding	United States	Reflects regulatory direction and expectations
Council of Europe Convention	Treaty Framework	Binding (for signatories)	Europe / International	Reinforces rights-based governance

Mapping Methodology and Alignment Scale

This methodology provides a structured approach for mapping AI systems against regulatory and governance frameworks. It ensures consistency, traceability, and audit readiness by guiding how obligations are identified, assessed, and documented across jurisdictions.

Alignment Scale Definitions

Strong Alignment

The system fully satisfies the requirement with clear, documented evidence and operational implementation in place.

Partial Alignment

The requirement is partially addressed, but gaps remain in documentation, implementation, or consistency.

Gap Identified

The requirement is not currently addressed. No sufficient controls, processes, or evidence exist.

Not Applicable

The requirement does not apply based on system scope, jurisdiction, or operational context.

Local Law Review Required

Further legal or regulatory analysis is required due to jurisdiction-specific obligations or uncertainty.

How to Apply the Scale

Each mapped obligation should be assessed using this scale. Assign a rating based on available evidence, implementation maturity, and regulatory expectations. Where gaps are identified, document remediation actions and assign ownership.

Jurisdiction and Organizational Applicability Matrix

This matrix helps organizations determine where and how AI systems are subject to regulatory obligations across jurisdictions. It supports structured assessment of deployment context, operational scope, and likely regulatory triggers.

Applicability Mapping Table

Jurisdiction	Business Unit	Deployment Context	System Type	User Impact	Likely Framework Trigger
EU	Product	Customer-facing AI	Recommendation System	Moderate	EU AI Act (Limited Risk)
United States	Engineering	Internal AI Tool	Automation System	Low	NIST AI RMF
Global	Compliance	Risk Monitoring AI	Decision Support	High	ISO/IEC 42001 + OECD Principles
EU	HR	Hiring AI Tool	Classification System	High	EU AI Act (High Risk)

How to Use This Matrix

Use this matrix to identify where AI systems operate and which regulatory frameworks are triggered. Each entry should reflect real deployment conditions, helping teams prioritize compliance actions and governance controls.

Governance Roles and Control Ownership

Define clear accountability across governance functions to ensure effective implementation, oversight, and continuous compliance with AI regulatory obligations.

Roles and Responsibilities Mapping

Role / Function	Key Responsibility	Ownership Type	Notes
Legal	Interprets regulatory obligations and ensures legal compliance alignment	Primary	Advises on jurisdiction-specific requirements
Compliance	Maps regulatory requirements to internal controls and monitors adherence	Primary	Owns governance framework implementation
Product Team	Ensures AI systems are designed in line with governance and risk requirements	Shared	Works closely with engineering and compliance
Engineering	Implements technical controls, logging, and system-level safeguards	Shared	Supports auditability and system transparency
Risk Management	Assesses AI risk levels and defines mitigation strategies	Primary	Aligns with enterprise risk frameworks
Security	Ensures data protection, access control, and system integrity	Shared	Works across infrastructure and product layers
Procurement / Vendor Management	Evaluates third-party AI systems and supplier compliance	Primary	Ensures vendor risk and contractual safeguards
Internal Audit	Reviews governance effectiveness and compliance readiness	Independent	Provides assurance and gap identification
Executive Sponsor	Provides strategic oversight and accountability at leadership level	Accountable	Ensures governance alignment with business strategy

Governance Principle

Effective AI governance depends on clearly defined ownership across legal, technical, and operational functions. Shared responsibility models must be reinforced with explicit accountability to prevent gaps in compliance and control execution.

Global AI Regulatory Mapping Table – Governance and Risk

This mapping table provides a structured approach to aligning governance and risk-related AI obligations across multiple regulatory frameworks. It supports consistent identification, classification, and oversight of AI systems.

Governance and Risk Mapping Table

Obligation Area	Description	EU AI Act	NIST AI RMF	OECD Principles	ISO/IEC 42001	Alignment Rating
Governance Structure	Establishment of internal AI governance frameworks and oversight mechanisms	Article 9 (Risk Management System)	Govern Function	Governance & Accountability	Clause 5 (Leadership)	Strong Alignment
Risk Identification	Identification of potential risks across AI system lifecycle	Article 9 (Risk Management System)	Map Function	Risk Awareness	Clause 6 (Planning)	Strong Alignment
Risk Assessment	Evaluation of severity and likelihood of identified risks	Article 9 (Risk Management System)	Measure Function	Risk Evaluation	Clause 8 (Operational Controls)	Strong Alignment
System Classification	Classification of AI systems based on risk categories	Articles 6–7	Map Function	Not Explicit Defined	Clause 8	Partial Alignment
Accountability Assignment	Clear allocation of responsibility for AI governance and compliance	Article 14	Govern Function	Accountability	Clause 5 (Leadership)	Strong Alignment
Human Oversight	Ensuring appropriate human involvement in AI decision-making	Article 14	Govern Function	Human-Centered Principles	Clause 8	Strong Alignment
Monitoring and Review	Continuous monitoring and periodic review of AI systems	Article 61	Manage Function	Lifecycle Responsibility & Oversight	Clause 9 (Performance Evaluation)	Strong Alignment

Interpretation Guidance

Each obligation area should be evaluated across frameworks to determine the level of alignment. Where partial alignment or gaps exist, organizations should document remediation actions, assign clear ownership, and ensure traceability to support audit readiness and regulatory compliance.

Global AI Regulatory Mapping Table – Documentation and Transparency

This mapping table focuses on documentation, transparency, and information disclosure obligations across major AI governance frameworks. It supports traceability, audit readiness, and clear communication of AI system behavior, risks, and controls.

Documentation and Transparency Mapping Table

Obligation Area	Description	EU AI Act	NIST AI RMF	OECD Principles	ISO/IEC 42001	Alignment Rating
Technical Documentation	Comprehensive documentation of AI system design, purpose, data, and risk controls	Article 11 (Technical Documentation)	Map + Govern Function	Transparency & Explainability	Clause 7 (Documented Information)	Strong Alignment
Recordkeeping	Maintenance of logs and records to ensure traceability of AI system operations	Article 12 (Recordkeeping)	Measure + Manage Function	Accountability	Clause 7.5 (Information Control)	Strong Alignment
Transparency	Clear communication that users are interacting with AI systems	Article 52 (Transparency Obligations)	Govern Function	Transparency	Clause 8 (Operational Transparency Controls)	Strong Alignment
User Disclosure / Notice	Providing users with appropriate information about system capabilities and limitations	Article 13 (Information to Users)	Govern + Map Function	Transparency & Responsible Disclosure	Clause 8 (Communication Controls)	Strong Alignment
Explainability	Ability to interpret and explain AI system outputs and decisions	Implicit (Articles 13–14 context)	Explainability (Map Function)	Explainability	Clause 8 (Model Transparency Practices)	Partial Alignment
Model and System Information	Documentation of model characteristics, performance, limitations, and intended use	Annex IV (Technical Documentation Details)	Map + Measure Function	Transparency & Accountability	Clause 7 + Clause 8	Strong Alignment

Interpretation Guidance

Organizations should ensure that all AI systems are supported by clear, structured documentation and transparent communication practices. Where explainability requirements are only partially addressed, additional controls and documentation should be implemented to strengthen audit readiness and stakeholder trust.

Global AI Regulatory Mapping Table – Controls and Monitoring

This mapping table focuses on operational controls, monitoring mechanisms, and lifecycle risk management practices required to ensure AI systems remain safe, fair, and compliant after deployment. It supports continuous oversight, incident response readiness, and regulatory accountability.

Controls and Monitoring Mapping Table

Obligation Area	Description	EU AI Act	NIST AI RMF	OECD Principles	ISO/IEC 42001	Alignment Rating
Bias and Fairness Controls	Implementation of measures to detect, mitigate, and monitor bias in AI systems	Article 10 (Data Governance)	Measure + Manage Function	Fairness	Clause 8 (Operational Risk Controls)	Strong Alignment
Testing and Validation	Pre-deployment and ongoing validation of system performance, safety, and reliability	Article 15 (Accuracy, Robustness, and Cybersecurity)	Measure Function	Robustness, Safety & Reliability	Clause 8 (System Validation Controls)	Strong Alignment
Human Oversight	Ensuring appropriate human involvement in AI system decision-making and intervention	Article 14 (Human Oversight)	Govern Function	Human-Centered Values	Clause 8 (Human Oversight Controls)	Strong Alignment
Incident Response	Processes for identifying, reporting, and responding to AI-related incidents and failures	Article 62 (Serious Incident Reporting & Corrective Actions)	Manage Function	Accountability	Clause 10 (Incident Management & Improvement)	Strong Alignment
Continuous Monitoring	Ongoing tracking of system performance, risks, and compliance throughout lifecycle	Article 61 (Post-Market Monitoring System)	Manage Function	Accountability & Lifecycle Oversight	Clause 9 (Performance Evaluation)	Strong Alignment
Post-Market Review	Periodic evaluation of AI systems after deployment to ensure continued compliance and safety	Article 61–63 (Monitoring & Corrective Actions)	Manage Function	Accountability & Lifecycle Oversight	Clause 9 + Clause 10	Strong Alignment

Interpretation Guidance

Organizations should implement strong operational controls and continuous monitoring mechanisms to ensure AI systems remain compliant throughout their lifecycle. Where risks evolve or incidents occur, timely response actions and structured review processes are essential to maintain regulatory alignment and system integrity.

Global AI Regulatory Mapping Table – Third Parties and Assurance

This section focuses on third-party risk management, assurance mechanisms, and independent oversight functions required for AI governance. It ensures that external dependencies, supplier risks, and audit readiness are properly controlled, monitored, and documented.

Third-Party and Assurance Mapping Table

Obligation Area	Description	EU AI Act	NIST AI RMF	OECD Principles	ISO/IEC 42001	Alignment Rating
Vendor Due Diligence	Assessment of third-party AI providers, including risk exposure, compliance posture, and governance maturity	Article 28 (Obligations for Providers & Third Parties)	Govern + Map Function	Accountability & Risk Management	Clause 8 (Operational Controls – Third-Party Management)	Strong Alignment
Contractual Controls	Inclusion of AI governance clauses in vendor contracts covering compliance, accountability, and audit rights	Article 28 + Article 16	Govern Function	Accountability	Clause 7.4 (Communication & Control of External Parties)	Strong Alignment
Conformity Assessment	Support for regulatory conformity assessments, CE marking, and compliance validation processes	Annex IV + Article 43	Measure + Manage Function	Accountability & Transparency	Clause 9 (Performance Evaluation & Audit)	Strong Alignment
Internal Audit	Independent evaluation of AI governance effectiveness, controls, and compliance readiness	Article 72 (Post-Market Monitoring & Review context)	Manage Function	Accountability	Clause 9.2 (Internal Audit)	Strong Alignment
Escalation	Defined processes for escalating risks, compliance breaches, and governance failures to leadership	Article 62 (Incident Reporting)	Manage Function	Accountability	Clause 10 (Improvement & Corrective Action)	Strong Alignment

Interpretation Guidance

Organizations must ensure that third-party relationships are governed with the same level of rigor as internal systems. Vendor risks, contractual obligations, and independent assurance mechanisms should be clearly defined, documented, and continuously monitored. Effective escalation and audit processes are essential to maintaining compliance and operational integrity.

Required Evidence and Artifacts Register

This register defines the evidence required to demonstrate compliance with AI governance obligations. It ensures that all regulatory requirements are supported by verifiable documentation, clearly assigned ownership, and traceable storage locations for audit readiness.

Evidence Register Table

Requirement	Evidence Type	Template / Source Document	Owner	Frequency	Storage Location	Status
Risk Management Framework	Risk Register, Risk Assessment Reports	Internal Risk Template / EU AI Act Article 9 Mapping	Risk / Compliance Team	Quarterly Review	Governance Repository (SharePoint / GRC Tool)	Active
AI System Classification	Classification Reports, Risk Categorization Logs	EU AI Act Articles 6–7 Classification Template	Compliance Team	On System Change	AI System Inventory Database	Active
Technical Documentation	Model Documentation, Design Specs, Data Descriptions	Annex IV (Technical Documentation Template)	Engineering / Product	Per Release	Technical Documentation Repository	Active
User Transparency Obligations	User Notices, AI Disclosures, UI Messaging	Article 52 Transparency Template	Product / Legal	Per Deployment	Product Documentation / Legal Repository	Active
Operational Logging	System Logs, Audit Trails	Logging Policy / ISO Control Template	Engineering / Security	Continuous	Logging Infrastructure (SIEM / Cloud Logs)	Active
Human Oversight Controls	Review Logs, Escalation Records	Human Oversight Procedure	Operations / Compliance	Continuous	Oversight Logs Repository	Active
Incident Management	Incident Reports, Monitoring Dashboards	Incident Response Plan	Security / Risk Team	As Occurs	Incident Management System	Active
Audit and Compliance Review	Audit Reports, Findings, Remediation Logs	Internal Audit Framework	Internal Audit	Annual / Periodic	Audit Repository	Active

Interpretation Guidance

A well-maintained evidence register is essential for demonstrating compliance during audits and regulatory reviews. Organizations should ensure that each requirement is backed by clear, accessible, and up-to-date documentation. Ownership must be defined, and evidence should be consistently maintained to support traceability and accountability across all AI systems.

Gap Assessment and Remediation Tracker

This tracker identifies gaps between current AI governance practices and regulatory requirements. It supports structured remediation planning by defining severity, ownership, timelines, and corrective actions to ensure compliance readiness.

Gap Assessment Table

Gap ID	Gap Description	Severity	Jurisdiction	Affected System	Owner	Target Date	Remediation Action	Review Status
GAP-001	Absence of documented AI risk management framework	High	EU	Customer-Facing AI System	Risk / Compliance	30 Days	Develop and implement risk management framework aligned with Article 9	In Progress
GAP-002	AI systems not formally classified under risk categories	High	EU / Global	All AI Systems	Compliance	14 Days	Conduct classification assessment using Articles 6–7	Not Started
GAP-003	Missing or incomplete technical documentation for AI systems	Medium	EU	AI Model Deployment Pipeline	Engineering	21 Days	Develop Annex IV compliant technical documentation	In Progress
GAP-004	Users not adequately informed about AI system usage	Medium	EU	User Interface / Application Layer	Product / Legal	14 Days	Implement user disclosure notices aligned with Article 52	Not Started
GAP-005	Lack of consistent logging and monitoring controls	High	Global	AI Operations Infrastructure	Engineering / Security	30 Days	Implement logging, monitoring, and audit trail systems	In Progress
GAP-006	Absence of structured incident response process for AI failures	High	EU / Global	All AI Systems	Security / Risk Team	21 Days	Develop incident response framework aligned with Article 62	Not Started

Interpretation Guidance

Gap assessment is a critical step in achieving regulatory compliance. Organizations should prioritize high-severity gaps and assign clear ownership to ensure timely remediation. Continuous tracking and periodic review of remediation actions are essential to maintaining alignment with evolving regulatory expectations.

Definitions and Interpretation Notes

This section defines key terms used throughout the AI governance framework to ensure consistent interpretation across teams, functions, and jurisdictions. Clear definitions reduce ambiguity and support accurate implementation of regulatory requirements.

Key Definitions

Provider

An organization that develops an AI system or places it on the market under its own name or trademark.

Deployer

An entity that uses an AI system in its operations, whether internally or in customer-facing environments.

High-Risk AI System

An AI system classified under regulatory frameworks (such as the EU AI Act) as posing significant risk to health, safety, or fundamental rights, requiring strict compliance obligations.

Human Oversight

Mechanisms that ensure human intervention, supervision, or control over AI system decisions where necessary.

Monitoring

Continuous observation and evaluation of AI system performance, risks, and compliance throughout its lifecycle.

Incident

Any event where an AI system causes or has the potential to cause harm, malfunction, or regulatory non-compliance.

Control Owner

The individual or function responsible for implementing, maintaining, and validating a specific governance control.

Evidence Artifact

Documented proof demonstrating that a control or requirement has been implemented and is functioning as intended.

Alignment Level

The degree to which a system, control, or process meets regulatory or governance requirements (e.g., strong, partial, gap).

Interpretation Notes

Organizations should apply these definitions consistently across all governance activities, documentation, and reporting processes. Where regulatory definitions differ across jurisdictions, the stricter interpretation should be adopted to ensure compliance and reduce risk exposure.

Final Review Checklist

Final Validation Checklist

Use this checklist to confirm that the AI governance mapping, documentation, and implementation framework is complete, consistent, and audit-ready.

Governance Readiness

- Legal review completed and regulatory interpretation confirmed
- Scope of AI systems clearly defined and validated
- Applicable jurisdictions identified and mapped
- Framework alignment (EU AI Act, NIST AI RMF, OECD, ISO/IEC 42001) verified

Ownership and Accountability

- Control owners assigned across all governance areas
- Roles and responsibilities clearly documented
- Executive oversight established and accountable
- Cross-functional coordination (legal, compliance, engineering, product) confirmed

Documentation and Evidence

- Technical documentation complete and up to date
- Evidence artifacts linked to each requirement
- Recordkeeping processes implemented and traceable
- Evidence storage locations defined and accessible

Risk and Control Implementation

- Risk management framework implemented and operational
- AI system classification completed and validated
- Control measures (bias, testing, oversight) implemented
- Human oversight mechanisms clearly defined

Monitoring and Lifecycle Management

- Continuous monitoring processes established
- Incident response procedures defined and tested
- Post-market monitoring and review processes active
- Performance evaluation and audit mechanisms in place

Gap Closure and Remediation

- All identified gaps documented in remediation tracker
- Severity levels assigned and prioritized
- Target dates defined and realistic
- Remediation actions actively tracked and updated

Review and Audit Readiness

Review and Audit Readiness

- Internal audit processes completed or scheduled
- Compliance status reviewed and validated
- Documentation prepared for regulatory inspection
- Evidence traceability confirmed across all controls

Final Note

Effective AI governance is not achieved through documentation alone, but through consistent implementation, ownership, and continuous monitoring. Organizations that maintain structured processes, clear accountability, and verifiable evidence will be best positioned for regulatory compliance and long-term operational trust.