

AI governance worldwide

Laws, ethics, frameworks and standards

What the world's AI governance instruments do
and what they leave to human judgment

GLOBAL REFERENCE REPORT

24 October 2026

Publication edition 3.0

About this publication

Published by Monforte Research
A research division of Monforte

This Monforte report maps the legal, ethical and technical instruments that shape AI governance worldwide. It explains what different forms of governance and assurance can establish, and where further evidence and accountable judgment are needed.

Publication date and disclaimer

This publication reflects information available and the sources reviewed as at 24 October 2026. Reasonable care has been taken to present that information accurately as at that date; completeness and continuing accuracy cannot be guaranteed. Laws, regulations, standards, guidance, proposals and implementation dates may change after publication. A proposal, publication, entry into force and the date an obligation becomes applicable are distinct events.

This report provides general research and analysis. It is not legal advice, a compliance opinion, an audit, a certification or an endorsement of any product, provider or deployment. Applicability depends on the jurisdiction, sector, organizational role and specific use. Readers should consult current official sources and appropriately qualified advisers before relying on the report for a decision.

Coverage and interpretation

The register is a selected worldwide map, not an exhaustive inventory of every jurisdiction or AI-related instrument. Some entries rely on official summaries rather than a full reading of consolidated legislation or licensed standards. The boundary column is Monforte's analysis of what the identified scope alone supports; it does not assert that the instrument never addresses the issue. The omission of a jurisdiction or instrument does not imply an absence of regulation.

Reader guide

Opening analysis • The central distinctions and legal force
Part A • International instruments and selected regional approaches
Legal duties beyond AI legislation • Existing obligations that still apply
Part B • Technical standards and assurance resources
Closing analysis • Choosing evidence for the decision

Use the three lenses of applicability, authority and evidence to read each entry. The opening distinctions explain common interpretation errors; the closing assurance questions apply them to an actual decision. Status labels belong to the reference date above.

Source links work in the downloaded PDF. A social-media document preview may display page images without active links. Download this report to open its linked official sources. The source review uses public texts, catalogues and official summaries; it is not a full-text audit of every licensed standard.

The central finding

AI governance worldwide is a layered landscape of binding laws, treaties, human-rights instruments, ethical declarations, public policies, supervisory guidance, standards and assurance methods. Each establishes a different kind of duty, expectation or evidence. Their differences in purpose, applicability and enforcement are central to understanding what they do and what they leave unresolved.

ISO/IEC 27090:2026, published on 14 October 2026, illustrates the distinction. It addresses threats and compromises to AI systems. Its security contribution sits alongside governance, management, impact, performance and legal instruments; it cannot serve as a single umbrella for the whole landscape.

Source: [ISO/IEC 27090 publication record](#)

How to read this register

The register begins with international ethics and human rights, regional instruments and selected national legal and policy approaches across Europe, North America, Latin America, Africa, Asia, the Middle East and the Pacific. It then retains the technical standards inventory and publication watchlist. It includes existing legal duties that can apply without using the term AI. National adoptions, overlapping frameworks and document families are not equivalent to separate laws.

Status and high-level scope were checked against official legislation, parliamentary dockets, issuing-body catalogues, regulator materials and public documents. Source depth varies: some records rely on official summaries rather than a full reading of consolidated legal text. This is a landscape review, not a country-specific legal opinion or a clause-by-clause examination of every instrument. The boundary column is analytical interpretation: it identifies conclusions that the listed scope alone cannot justify. It should not be read as an assertion that a standard never mentions the subject.

Each document name links to its primary source. “Published” describes availability, not legal obligation. IS = International Standard; TS = Technical Specification; TR = Technical Report; PAS = Publicly Available Specification. CD, DIS and FDIS denote development stages. A TS can contain requirements; a TR is primarily informative. Certification depends on the document, scheme, scope and assessment body—not on the word “standard” alone.

Five distinctions that matter

- Governing AI versus operating an AI management system.
- Managing risk versus assessing impacts on people and society.
- Protecting an AI system versus proving its outputs are suitable for a task.
- Conformity of a management system versus conformity of an AI product or deployment.
- Voluntary guidance versus a standard given a specific role by law or contract.

The worldwide map of legal force

AI governance instruments do different jobs. Some establish duties, others articulate values, guide public administration, organize controls or supply evidence. Their relevance depends on the organization's role, the people affected, the location of use and the market served—not simply where its head office is located.

Instrument and status	What it contributes	What it does not establish by itself
Binding laws and regulations Jurisdiction-specific	Prohibit, require, authorize, allocate liability or provide rights and remedies.	A standard or policy cannot waive an applicable legal obligation.
Treaties Party-specific	Create international obligations, often requiring domestic implementation.	Signature, ratification, entry into force and direct domestic effect are different questions.
Regulatory guidance / public policy Force depends on issuing power and audience	Interpret duties or direct supervised/public bodies.	An opinion, government strategy and enforceable regulation are not interchangeable.
Ethics and human rights frameworks Normative / due-diligence reference	Identify affected people, values, participation, remedy and acceptable conduct.	Voluntary status does not make ethical concerns irrelevant; endorsement does not prove implementation.
Standards and assurance schemes Normally voluntary; may be incorporated elsewhere	Specify systems, processes, controls, tests or assessment arrangements.	Certification has a defined object, scope and evidential boundary.

Three lenses for every entry

Applicability: which actor, activity, person, market and territory trigger it? Force: is it binding law, treaty duty, administrative policy, supervisory expectation, voluntary guidance or a proposal? Evidence: what must be demonstrated, to whom, by whom and at what point in the life cycle?

Worldwide does not mean universally applicable

This worldwide map uses selected national examples across regions. It is not an exhaustive statement of every statute, court judgment, provincial law or agency rule. A country's absence is not evidence that AI is unregulated there. The OECD Policy Navigator provides additional country-level discovery resources.

Discovery source: [OECD national policy repository](#)

Part A legal ethical and regional instruments

A1 International instruments and regional policy

Instrument and status	What it contributes	What it does not establish by itself
Council of Europe AI Framework Convention (CETS 225) Treaty • entry into force pending	Establishes a treaty framework for rights, democracy and rule-of-law safeguards. The EU ratified on 15 May 2026.	Signature is not ratification. Entry into force requires five ratifications, including three Council of Europe member states; domestic implementation and party scope remain distinct.
UN Guiding Principles on Business and Human Rights / OHCHR B-Tech Global normative framework • not an AI certification	Human-rights due diligence, business responsibility, remedy and technology-specific application.	Principles do not themselves establish a new globally enforceable corporate cause of action.
UN Global Digital Compact (2024) Global political commitment • not a treaty	Cooperation on digital inclusion, rights, data governance and international AI governance.	A political commitment is not a directly enforceable compliance regime for all companies.
G7 Hiroshima AI Process principles and code Voluntary • advanced-AI developers and wider AI actors	International principles and development practices for safe, secure and trustworthy advanced AI.	Endorsement is not regulatory approval, independent verification or a universal law.
African Union Continental AI Strategy (2024) Adopted regional strategy • not continent-wide corporate law	Africa-centered, development-oriented AI, inclusion, capability building and risk governance.	Member states still require their own implementation; the strategy does not harmonize all national laws.
ASEAN AI Governance and Ethics Guide / GenAI expansion Regional voluntary guidance • 2024 / 2025	Organizational governance and regional cooperation, expanded to generative-AI risks.	It does not replace individual ASEAN members' laws or create a common licensing regime.

A2 Ethics and human rights

Instrument and status	What it contributes	What it does not establish by itself
UNESCO AI Ethics Recommendation / RAM Global recommendation • implementation tools	Rights, dignity, social and environmental concerns; readiness assessment of national institutions and capacity.	Country readiness does not validate a model or establish that a deployment is ethically acceptable.
Council of Europe HUDERIA / COBRA Non-binding methodology • approvals 2025 / 2026	Context-based assessment of risks and impacts on human rights, democracy and rule of law.	It is not mandatory solely because the AI Convention exists, nor a substitute for the applicable law.
UNICEF Guidance on AI and Children 3.0 Global guidance • December 2025	Child-rights approach for governments and businesses designing AI policies and systems.	It is not a child-safety certificate; existing child-protection duties still require jurisdictional analysis.
WHO AI ethics and governance guidance for health / LMMs Global health guidance • 2021 and 2024	Ethical governance of health AI and large multimodal models in clinical and health-related uses.	WHO guidance is not national market authorization, clinical validation or a medical-device approval.
Toronto Declaration (2018) Civil-society declaration • Amnesty / Access Now	Equality, non-discrimination, participation and access to remedy in machine learning.	It is a normative declaration, not legislation or a complete technical testing specification.
Montreal Declaration for Responsible AI Voluntary ethical declaration	Values including autonomy, well-being, justice and democratic participation inform responsible AI choices.	Signing or citing it does not demonstrate implementation or resolve conflicts among values.
Rome Call for AI Ethics (2020) Voluntary multi-stakeholder commitment	Human dignity, inclusion, accountability, impartiality, reliability, transparency, security and privacy.	An ethical commitment is not an audit conclusion or legal compliance determination.

A3 Europe

Instrument and status	What it contributes	What it does not establish by itself
EU AI Act, Regulation 2024/1689, as amended Binding regulation • amended by Regulation (EU) 2026/1744	Risk-based AI duties. Most rules apply from 2 August 2026, including transparency duties subject to transitions. Main high-risk milestones: 2 December 2027 (Annex III) and 2 August 2028 (Annex I).	Applicability depends on actor, system, territory, exceptions and transitions. The December 2026 milestone includes new prohibited uses and a synthetic-content marking transition; there is no single compliance date for every duty.
EU GPAI Code of Practice Voluntary compliance-support tool under the AI Act	Helps GPAI providers demonstrate compliance in transparency, copyright, safety and security.	Voluntary code participation does not make statutory obligations optional or establish every downstream use is compliant.
GDPR / EDPB automated decision-making guidance Binding data law • guidance interprets duties	Lawful processing, data rights, profiling and safeguards for specified significant automated decisions.	Data-protection compliance is not a complete judgment on non-personal-data harms, performance or sector safety.
Digital Services Act Binding regulation • covered intermediary services	Platform obligations, including systemic-risk duties for designated very large services; relevant to AI-mediated content.	It is not a general law governing every enterprise AI system.
Cyber Resilience Act Binding regulation • reporting began September 2026	Cybersecurity of covered products with digital elements; main obligations apply from December 2027.	Coverage depends on product and exceptions; it does not settle broader social and ethical acceptability.
Revised Product Liability Directive 2024/2853 Adopted directive • national implementation due December 2026	Modernizes defective-product liability, including software and AI-enabled products.	It is not a pre-deployment approval. National transposition and temporal application matter.
Platform Work Directive 2024/2831 Adopted directive • national implementation required	Algorithmic-management transparency, human oversight and worker protections in platform work.	It is not a general rule for every employee or every workplace AI application.

A4 United Kingdom and Canada

Instrument and status	What it contributes	What it does not establish by itself
UK data-protection law / Data (Use and Access) Act 2025 Binding law • amended automated-decision rules	Personal-data processing and safeguards for significant automated decisions; use current amended provisions.	Do not assume the former UK GDPR Article 22 wording remains unchanged or that all AI is in scope.
DPA 2018 AI and Automated Decision-Making Code Regulations 2026 (SI 2026/425) In force 12 May 2026 • direction to the Information Commissioner	Requires preparation of a code on personal-data processing in developing and using AI and automated decision-making, including children's data.	The regulations are not the completed ICO code. Their commencement does not mean that the future code is already applicable.
UK Algorithmic Transparency Recording Standard Mandatory government policy within defined scope	Publication of records about covered public-sector algorithmic tools; voluntary adoption outside mandatory scope.	Publishing a record is not approval of the tool or proof that its decisions are fair.
UK Data and AI Ethics Framework Government guidance • updated December 2025	Supports ethical public-sector data and AI use, accountability and transparency.	It does not displace public law, equality law, data protection or sector regulation.
Canada Directive on Automated Decision-Making / AIA Mandatory federal administrative policy within scope	Impact assessment, transparency, quality and recourse for covered departmental administrative decisions.	Not a general private-sector AI law, and not all federal AI use is covered.
Canada AIDA / Bill C-27 Proposal-history entry • not an enacted AI Act	Illustrates proposed regulation of high-impact AI; retain separately from current obligations.	An official explanatory page using “would” is not evidence that the proposal became law.
Canada Bill C-36 on privacy and consumer data Introduced 15 June 2026 • proposed legislation	Proposes private-sector privacy reform, including protections concerning automated decisions.	A bill is not operative law. It is not an enacted replacement for AIDA or a comprehensive AI licensing regime.

A5 United States federal law and policy

Instrument and status	What it contributes	What it does not establish by itself
US Title VII / employment-discrimination law Binding law • covered employers	Existing employment protections apply when AI assists employment decisions; vendor use does not remove employer duties.	A narrow bias audit or vendor certificate does not establish compliance with every employment-law duty.
US FTC Act, section 5 Binding consumer-protection statute	Section 5 prohibits unfair or deceptive acts or practices within the FTC's jurisdiction, including applicable AI marketing and conduct.	The statute is distinct from proposed enforcement policy. A policy proposal does not establish enacted preemption or create universal AI approval.
US TAKE IT DOWN Act Enacted 2025 • covered platforms and conduct	Addresses non-consensual intimate imagery, including AI deepfakes, and covered-platform removal duties.	It does not regulate all synthetic content, all misinformation or every AI service.
US Executive Order 14179 Signed 23 January 2025 • federal executive policy	Directs federal AI policy and development of an action plan to advance US AI leadership.	An executive policy direction is not a comprehensive private-sector AI statute and does not itself resolve every state-law obligation.
America's AI Action Plan and July 2025 orders Plan and EOs 14318 to 14320 • 23 July 2025	Combines innovation policy, data-center permitting, federal procurement conditions and exports of US AI technology.	The plan and the individual executive orders have different legal roles. Industrial policy is not an independent ethics assessment or proof of product safety.
US Executive Order 14365 Signed 11 December 2025 • federal-state AI policy	Directs federal action on perceived state-law barriers, including litigation and regulatory initiatives concerning AI.	An executive instruction to challenge state laws does not establish that each law is invalid or that a proposed preemption position has prevailed.
OMB M-25-21 and M-25-22 Issued 3 April 2025 • federal agency use and acquisition	Sets federal requirements for AI use, governance and procurement. The memoranda replace earlier use and acquisition policies.	Federal agency policy is not a universal certification scheme for commercial AI or a substitute for applicable statutes.
FTC proposed policy on suppression of AI accuracy Proposed 1 July 2026 • not a final policy in the source reviewed	Proposes an approach to Section 5 and AI accuracy representations; raises a state-law preemption argument in the EO 14365 policy context.	A proposed interpretation is not enacted law, a final enforcement policy or a judicial determination that state AI duties are preempted.

A6 United States state and local measures

Instrument and status	What it contributes	What it does not establish by itself
California SB 53 / TFAIA Enacted September 2025 • frontier-model developers	Public safety frameworks, critical-incident reporting and whistleblower protections for covered actors.	Not certification of all AI products, and not the vetoed SB 1047.
Colorado SB 26-189 on consequential automated decisions Signed 14 May 2026 • principal duties from 1 January 2027	Replaces the earlier framework with duties concerning automated decision-making technology in consequential decisions, including discrimination and consumer protections.	Do not rely on an unchanged SB 24-205 summary or assume the future compliance date has already passed.
New York City Local Law 144 Binding local law • covered employment decision tools	Independent bias audits, public audit information and notices for covered tools and uses.	The audit has a defined scope; it is not blanket validation of job relevance, legality or fairness.
Texas HB 149 Texas Responsible AI Governance Act • effective 1 January 2026	Sets specified prohibited AI uses, enforcement provisions and state governance arrangements.	The law has its own definitions and exclusions; it is not equivalent to the EU AI Act or an assessment of every AI risk.
Illinois HB 3773 / Public Act 103-0804 Human Rights Act amendments • effective 1 January 2026	Addresses discriminatory AI use and notice in covered employment decisions.	Compliance requires the employment context and protected rights to be assessed; a generic bias metric does not resolve the full duty.
California CCPA ADMT and related regulations Effective 1 January 2026 • compliance dates vary by duty	Adds automated-decision rights, risk-assessment and cybersecurity-audit requirements within the CCPA's scope.	Commencement and operational compliance dates are distinct. ADMT duties have a 1 January 2027 milestone; other requirements have separate schedules.
California employment ADS regulations Civil Rights Council regulations • effective 1 October 2025	Applies employment discrimination protections to automated decision systems and associated practices.	A vendor's technical test or a privacy assessment does not itself demonstrate compliance with employment discrimination duties.
California SB 243 companion chatbots Enacted October 2025 • safeguards with phased requirements	Requires specified disclosures and safeguards for covered companion-chatbot interactions, with particular attention to minors and self-harm.	A chatbot-specific law does not govern every AI application; the text and dates of individual obligations must be checked.
California AB 2013 training-data transparency Enacted 2024 • disclosures due from 1 January 2026	Requires covered generative-AI developers to publish specified training-data documentation.	Disclosure does not establish copyright permission, dataset quality or lawful processing for every training input.

A7 East and Central Asia

Instrument and status	What it contributes	What it does not establish by itself
China Generative AI Interim Measures Binding departmental measures • effective August 2023	Providers serving the domestic public: content, data, rights and governance obligations, with specified assessments/filing.	Do not assume all internal AI development is governed identically or that compliance is globally portable.
China AI-generated/synthetic-content labelling measures Binding measures • effective September 2025	Explicit and implicit labels and responsibilities across generation and distribution; linked mandatory technical standard.	Labelling does not establish truth, lawful source data, fairness or safety of every output.
China anthropomorphic AI interaction measures Binding measures • effective July 2026	Target sustained emotional interaction, user dependency, minors and provider safety responsibilities.	Do not extend their scope to every chatbot; ordinary assistance without sustained emotional interaction is distinguished.
China Algorithmic Recommendation Provisions Binding departmental provisions • effective 1 March 2022	Regulates covered algorithmic recommendation services, including user rights, governance and filing obligations for specified services.	Scope and filing triggers are service-specific; the provisions are not a universal product certification or a complete statement of all Chinese AI law.
China Deep Synthesis Provisions Binding provisions • effective 10 January 2023	Addresses covered synthetic-content services, including identity, security, labeling and applicable filing requirements.	The provisions apply alongside other content, cybersecurity and personal-information rules; compliance with one instrument does not establish compliance with all.
China Cybersecurity Law amendment Amended law • effective 1 January 2026	New Article 20 addresses AI development, infrastructure, ethics, risk monitoring and security oversight within the cybersecurity framework.	A statutory policy provision is not a complete implementing code for every AI use or a global ethics certification.

A7 East and Central Asia — Continued

Instrument and status	What it contributes	What it does not establish by itself
Republic of Korea AI Basic Act / Enforcement Decree In force January 2026 • implementation/grace arrangements	AI development and trust framework; transparency, high-impact AI and safety obligations.	It is distinct from the EU model. Entry into force and enforcement/grace arrangements are different questions.
Japan AI Act, Act 53 of 2025 In force • fully commenced September 2025	Promotes AI R&D and use, national coordination and appropriate governance.	Do not describe its primarily promotional framework as an identical equivalent of EU high-risk regulation.
Japan Article 13 appropriateness guideline Decided 19 December 2025 • provisional English translation January 2026	Guides appropriate AI research, development and use under Article 13 of the AI Act, covering businesses, government and citizens.	Distinct from the METI/MIC AI Guidelines for Business. Guidance under a statute is not interchangeable with an independently enforceable duty for every recommendation.
Taiwan AI Basic Act Promulgated January 2026 • framework law	Human-centered AI, rights, government duties and risk-based regulatory development.	Framework legislation does not mean every sectoral obligation or implementing mechanism is already complete.
Kazakhstan Law 230-VIII on Artificial Intelligence Enacted 2025 • effective January 2026	National framework for AI development and use, safety, transparency and accountability.	Official legal-research summary supports identification; check the consolidated national text and later amendments for deployment advice.
Japan AI Guidelines for Business version 1.2 METI/MIC • voluntary guidelines • March 2026	Business-oriented governance principles and practices for AI developers, providers and users across the life cycle.	Separate from the Cabinet Office Article 13 guideline; following voluntary practices alone does not establish compliance with every applicable law.

A8 South and Southeast Asia

Instrument and status	What it contributes	What it does not establish by itself
India AI Governance Guidelines Government guidelines • launched November 2025	Principles-based governance, institutional coordination and responsible adoption across sectors.	The guidelines do not replace existing legislation or create a single omnibus AI licensing law.
Viet Nam Law on Artificial Intelligence Law 134/2025/QH15 • effective March 2026	National AI framework, responsibilities, risk management, transparency and governance; transition provisions apply.	A national AI strategy and an enforceable law are different instruments; implementing rules and timing still matter.
Singapore PDPA / AI advisory guidance Binding data law • interpretive AI guidance	Personal-data responsibilities apply to AI recommendation/decision systems, including identifiable derived data.	Advisory guidance is not a separate AI Act and does not settle all non-data harms.
Singapore MAS AI Risk Management Guidelines Final October 2026 • effective from October 2027	Supervisory expectations for financial institutions' AI governance, risk systems and life-cycle controls.	Not a cross-sector statute. Future effective and phased adherence dates must not be treated as current deadlines.
Malaysia proposed AI Governance Bill Consultation launched 10 July 2026 • proposal	Consults on a national governance framework for responsible AI development, deployment and use.	Consultation material is not an enacted statute. Proposed duties and institutional arrangements may change.
Indonesia proposed AI ethics and roadmap regulations Draft presidential regulations • official May 2026 development notice	Develops national AI ethics and a 2026–2029 roadmap through interministerial coordination.	The cited notice concerns draft completion, not proof of promulgation. No binding force is inferred from the proposal.

A9 Latin America

Instrument and status	What it contributes	What it does not establish by itself
Peru Law 31814 / Supreme Decree 115-2025-PCM Law and implementing regulation • regulation adopted September 2025	AI development and use with governance, risk and ethical safeguards under the national framework.	The framework does not confer international certification or replace sector/privacy obligations; phase-in needs checking.
Colombia SIC Circular 002/2024 Regulatory instructions • supervised data-processing actors	Clarifies personal-data duties in developing, deploying and using AI.	A data regulator's circular is not a comprehensive statute governing every dimension of AI.
Colombia CONPES 4144/2025 Approved national policy • government roadmap	Ethics/governance, infrastructure, capability building, adoption and risk mitigation through coordinated policy.	A national policy roadmap is not a general private-sector AI liability or licensing statute.
Brazil PL 2338/2023 Pending in the Chamber of Deputies as at 24 October 2026	Proposed broad AI rights and governance regime; official docket remains the status authority.	Senate approval, a draft text or continued debate does not establish enactment.

A10 Africa

Instrument and status	What it contributes	What it does not establish by itself
Kenya AI Strategy 2025–2030 Adopted national strategy • governance roadmap	Infrastructure, data, innovation and governance with inclusion and capacity-building objectives.	Strategy adoption does not itself enact every proposed control or override data-protection law.
Nigeria National AI Strategy National strategy • 2025 official publication	Responsible, ethical and inclusive adoption, capability and socioeconomic development.	A strategy is not an all-purpose AI statute or proof of enforcement capacity.
Rwanda National AI Policy National policy • adopted framework	Responsible innovation, development and ethical precautions tailored to Rwanda.	Policy ambitions do not establish product approval or replace applicable national laws.
South Africa POPIA, including section 71 Binding personal-information law	Personal-data protection and specified automated decision-making safeguards apply independently of a dedicated AI law.	A withdrawn AI policy does not remove existing duties, nor does POPIA cover every AI consequence.
South Africa 2026 draft AI policy Withdrawn • official notice June 2026	Historical policy-development document; retain withdrawal record for status accuracy.	It is neither current adopted policy nor an enforceable national AI statute.
Egypt National AI Strategy 2025–2030 Second edition • launched 22 January 2025	National development and governance strategy supporting skills, adoption and the Digital Egypt agenda.	A strategy is not a general AI licensing law or evidence that an individual deployment respects affected people's rights.

A11 Middle East and Pacific

Instrument and status	What it contributes	What it does not establish by itself
Saudi SDAIA AI Ethics Principles Ethics framework • application depends on instrument/context	Fairness, human interests, privacy/security, reliability, transparency and accountability.	Do not assume identical legal force for public guidance, agency requirements and underlying binding laws.
Saudi government GenAI guidelines Government guidance • public-entity responsibilities	Tool-specific governance, ethical safeguards and life-cycle responsibilities for government use.	Government-directed requirements are not automatically an equivalent private-sector AI statute.
Dubai Ethical AI Toolkit Ethical guidance / self-assessment • local application	Fairness, accountability, transparency and explainability with practical self-assessment.	Self-assessment is not independent certification. Agency adoption can create narrower mandatory requirements.
CBUAE guidance on consumer protection and responsible AI and ML Rulebook issued 11 February 2026 • announcement 23 February 2026	Sets supervisory principles for AI/ML use affecting consumers by licensed financial institutions, including insurers.	Financial-sector guidance does not constitute universal AI certification or replace other applicable financial and consumer duties.
Australia Guidance for AI Adoption / AI6 Voluntary guidance • implementation document dated October 2025	Six responsible AI practices covering accountability, impacts, risk, information, testing and human control.	It is not mandatory merely because government issued it; existing applicable laws still bind.
New Zealand Public Service AI Framework Public-service framework • published guidance	Lawful, responsible public-service AI informed by rights, public values and the national context.	Not a universal private-sector certification. Māori interests and applicable legal duties need contextual assessment.
UAE Charter for the Development and Use of AI National policy charter • 2024	Guiding framework for responsible AI development and use, aligned with the UAE's AI strategy.	A policy charter does not itself establish a universal product approval scheme or displace binding sector regulation.

A12 Sector regulation

Instrument and status	What it contributes	What it does not establish by itself
US FDA AI-device PCCP guidance Final guidance • current FDA page August 2025	Recommendations for predetermined change control plans in submissions for AI-enabled device software functions; the guidance was first finalized in December 2024.	A plan is not general approval of AI; device status, submission and authorized modifications matter.
EIOPA AI governance and risk opinion Supervisory opinion • August 2025 • EU insurance	Clarifies existing insurance-sector governance expectations for AI and supports supervisory convergence.	An opinion addressed to supervisors is not the same instrument as a new directly applicable AI regulation.
US Copyright Office AI reports Parts 1 and 2 final • Part 3 pre-publication version 9 May 2025	Analyses digital replicas, copyrightability and generative-AI training. Each part has its own publication status.	Reports are not legislation or binding court decisions. Part 3 must not be described as a final report or a universal permission to use training data.

Legal duties beyond AI legislation

Privacy, confidentiality and data transfers

Identify lawful processing, transparency, sensitive data, rights and cross-border transfer rules. GDPR, UK law, Singapore PDPA and South Africa POPIA illustrate different legal contexts.

Equality, employment and worker participation

Check hiring, promotion, dismissal, disability accommodation, surveillance, consultation and collective rights. A narrow statistical bias test may address only one part of the duty.

Consumer protection and competition

Assess misleading performance claims, manipulation, unfair conduct, vulnerable users, market power and conflicts of interest. “AI-powered” is not an exemption.

Product safety and professional duties

Identify the intended use and regulated product or service. Healthcare, transport, financial services and critical infrastructure impose requirements beyond generic AI governance.

Copyright, trade secrets and ownership

Check rights in training inputs, retrieval sources, prompts, outputs, likeness and voice. No universal conclusion on training permissions follows from a general AI standard.

Public law, rights and remedies

Public-sector decisions can engage legality, procedural fairness, reasons, review, accessibility and constitutional or human-rights protections.

Children, disability and affected communities

Consider age-appropriate design, accessibility, dependency, exclusion, participation, language and culturally specific impacts. “Average user” testing can miss those affected.

Security, environment and supply chains

Examine operational resilience, supplier dependencies, incident reporting, energy and water impacts, procurement obligations and applicable environmental rules. Technical AI controls do not replace local permits or organizational responsibilities.

Contracts, procurement and professional commitments

Voluntary documents can become binding between parties when incorporated into contracts or purchasing conditions. Check the exact promise and assessment scope rather than assuming global equivalence.

What the worldwide landscape reveals

The problem is not just a shortage of standards

The worldwide landscape combines different purposes: industrial development, national security, individual rights, ethical commitments, institutional accountability, product safety and technical assurance. Shared words such as “fairness” or “transparency” do not establish identical duties, values, enforcement or remedies. These differences deserve examination rather than being flattened into a common checklist.

A system can satisfy a management-system standard yet still require separate legal, clinical, employment or public-law scrutiny. A lawful use can still raise an unresolved ethical question. An ethical policy can still lack a workable test, an accountable decision-maker or an accessible remedy. These are distinct questions about the deployment, not reasons to dismiss the instruments.

Five questions for comparing instruments

- The people and interests the instrument protects.
- The actor responsible: developer, provider, deployer, employer, public authority or platform.
- The type of authority: law, treaty, supervisory expectation, ethics, contractual promise or technical standard.
- The evidence and enforcement mechanism: disclosure, impact assessment, independent audit, regulator, court or self-assessment.
- The boundary: exclusions, transition periods, national implementation and decisions still left to the organization.

Before relying on an assurance claim

Identify what was assessed, against which criteria, within what scope, using what evidence, and what decision that evidence supports. Governance of an organization, conformity of a management system, model performance and the effects of a deployment are related subjects. Assessment of one does not automatically establish the properties of the others.

The practical task is to connect applicable duties, ethical commitments and technical evidence to an accountable decision. Where the evidence ends, the organization must make the remaining judgment explicit and retain responsibility for it.

Status changes that illustrate the need for a dated map

Publication, entry into force and the date a duty applies must be recorded separately. The EU AI Act has staggered milestones through 2028. Colorado’s replacement statute has principal duties starting in January 2027; South Africa’s 2026 draft policy was withdrawn; Brazil’s bill remains pending. These different states should never be flattened into a single label of “AI regulation”.

[EU implementation timeline](#) | [Colorado legislature](#) | [South Africa withdrawal notice](#) | [Brazil parliamentary docket](#) | [MAS final guidelines](#)

Technical standards and assurance resources

Technical standards and assurance resources sit alongside legal duties and ethical commitments. The OECD AI Principles and UNESCO Recommendation are intentionally repeated here because they inform operational governance as well as public policy. They retain their original normative status in both listings.

B1 Governance management risk and impact

Instrument and status	What it contributes	What it does not establish by itself
ISO/IEC 38507:2022 Published • governance guidance	Helps governing bodies direct and oversee organizational use of AI.	An operating control system, product approval or release decision.
ISO/IEC 42001:2023 Published • AIMS requirements	Requirements for establishing, maintaining and improving an AI management system; supports management-system certification.	That every model is accurate, every use is acceptable, or every deployment is legally compliant.
ISO/IEC 23894:2023 Published • risk guidance	Adapts risk management to organizations developing, providing, deploying or using AI.	Universal risk tolerances, a complete risk register or an automatic certification route.
ISO/IEC 42005:2025 Published • impact guidance	Structures AI system impact assessment across foreseeable applications and the life cycle.	That identifying an impact resolves it, or that an assessment automatically satisfies a statutory assessment duty.
ISO/IEC 42006:2025 Published • certification-body requirements	Additional requirements for bodies auditing and certifying AI management systems against ISO/IEC 42001.	Certification of an individual model, nor a substitute for product evaluation.
ISO 31000:2018 Published • general risk guidance	Guidelines for enterprise risk principles, framework and process. A third-edition revision is under development; the published 2018 edition remains a separate document.	AI-specific testing, technical controls or prescriptive acceptable-risk thresholds.
ISO 37000:2021 / ISO/IEC 38500:2024 Published • wider governance	Organizational governance and governance of IT provide the surrounding governance context.	The detailed AI engineering and operational evidence needed for a particular use.

B2 Security and privacy

Instrument and status	What it contributes	What it does not establish by itself
ISO/IEC 27090:2026 Published 14 October 2026 • guidance	AI-specific threat identification, detection and mitigation across the life cycle; complements 27001/27002.	An all-purpose AI governance system or proof that an uncompromised AI makes sound decisions.
ISO/IEC 27001:2022 Published • ISMS requirements; amendment exists	Requirements for managing information security within a defined organizational scope.	AI-specific coverage merely because a supplier holds an ISMS certificate.
ISO/IEC 27002:2022 Published • security control guidance	Reference controls supporting information security management.	An independent management-system certification or a complete AI risk treatment.
ISO/IEC 27701:2025 Published • independent PIMS requirements	Privacy management for PII controllers and processors; second edition replaces the 2019 edition.	Lawfulness of every AI data use, nor automatic compliance with privacy legislation.
ETSI EN 304 223 V2.1.1 Published • December 2025	Baseline cybersecurity requirements for AI models and systems, including generative AI, across the life cycle.	Coverage of all AI harms or automatic EU AI Act harmonized status.
NIST SP 800-218A Final • July 2024 • SSDF profile	Secure development practices for generative AI and dual-use foundation models, used with the SSDF.	A complete governance, social-impact or task-validity assessment.
NIST AI 100-2 E2025 Final • adversarial ML taxonomy	Common vocabulary for attacks and mitigations involving machine learning.	A full control implementation, exhaustive threat coverage or proof of resistance.

B3 Life cycle terminology and data quality

Instrument and status	What it contributes	What it does not establish by itself
ISO/IEC 22989:2022 Published • concepts and terminology	Common AI vocabulary. The generative-AI amendment is a final draft amendment (FDAmD 1), not a published amendment.	Operational controls, safety assurance or a certification scheme.
ISO/IEC 23053:2022 Published • ML system framework	Framework describing AI systems using machine learning. Its generative-AI amendment is also at final draft amendment stage.	Validation of a particular architecture or application.
ISO/IEC 5338:2023 Published • AI life cycle processes	Processes for AI development, acquisition, operation and improvement, building on system/software life cycles.	The evidence that a completed process produced a sufficiently safe or useful result.
ISO/IEC 8183:2023 Published • data life cycle	Framework for organizing data across an AI system's life cycle.	Data ownership rights, representativeness or quality merely from following the stages.
ISO/IEC 5259-1:2024 Published • data quality foundation	Overview and terminology for data quality in analytics and ML.	Actual fitness of a particular dataset.
ISO/IEC 5259-2:2024 Published • data quality measures	Measures for describing and assessing data quality.	Which quality level is sufficient for a specific decision.
ISO/IEC 5259-3:2024 Published • requirements and guidance	Management of data quality for analytics and ML.	Absence of harmful bias or downstream decision error.
ISO/IEC 5259-4:2024 Published • process framework	Processes for implementing data quality management.	That a process record demonstrates successful real-world performance.
ISO/IEC 5259-5:2025 Published • data quality governance	Governance framework for analytics/ML data quality.	Permission to use data or a complete AI governance system.
ISO/IEC TR 5259-6:2026 Published • technical report	Visualization framework for data quality.	That a clear visualization proves adequate data quality.

B4 Testing robustness and performance

Instrument and status	What it contributes	What it does not establish by itself
ISO/IEC 25059:2023 Published • revision at FDIS	AI system quality model to structure requirements and evaluation.	A universal pass mark or actual achievement of the quality characteristics.
ISO/IEC TS 25058:2024 Published • revision project active	Guidance for evaluating AI system quality.	That an evaluation generalizes to every population, integration or future update.
ISO/IEC TS 42119-2:2025 Published • AI testing	Requirements and guidance applying software testing practices to AI on a risk basis.	Discovery of every failure mode, or product acceptance without defined criteria.
ISO/IEC TS 4213:2022 Published • revision in development	Assessment of machine learning classification performance.	Equivalent evidence for all regression, recommendation or generative-AI tasks.
ISO/IEC TR 24029-1:2021 Published • robustness overview	Concepts for assessing neural-network robustness.	A robustness guarantee or a complete operational safety case.
ISO/IEC 24029-2:2023 Published • formal-method methodology	Use of formal methods in neural-network robustness assessment.	Claims beyond the formalized properties, assumptions and evaluated model.
ISO/IEC TR 42106:2026 Published • differentiated benchmarking	Overview of differentiated benchmarking of AI system quality characteristics.	That one benchmark score establishes fitness for a different use context.
ISO/IEC TS 42112:2026 Published • training efficiency	Guidance for optimizing ML model training efficiency.	Acceptable social impact or dependable operational decisions.

B5 Transparency bias and societal effects

Instrument and status	What it contributes	What it does not establish by itself
ISO/IEC TR 24027:2021 Published • bias overview	Sources and considerations of bias in AI and AI-assisted decisions.	A universally correct definition of fairness or a bias-free system.
ISO/IEC TS 12791:2024 Published • bias treatment	Techniques addressing unwanted bias in ML classification and regression throughout the life cycle.	All forms of societal discrimination or validation of unrelated generative tasks.
ISO/IEC TR 24028:2020 Published • trustworthiness overview	Shared discussion of AI trustworthiness and associated approaches.	A single operational trust score or proof that a system deserves reliance.
ISO/IEC 12792:2025 Published • transparency taxonomy	Information elements relevant to different stakeholders' transparency needs.	That disclosure is understandable, sufficient for challenge, or evidence of correctness.
ISO/IEC TS 6254:2025 Published • explainability guidance	Approaches to explainability and interpretability matched to stakeholder objectives.	A causal explanation or a justified decision merely because an explanation is available.
ISO/IEC TS 8200:2024 Published • controllability	Framework for observing system state, transferring control and handling uncertainty.	That a nominal human reviewer has the time, competence and authority to intervene.
ISO/IEC TR 24368:2022 Published • ethics and society	Overview of ethical and societal concerns associated with AI.	Resolution of competing values or authorization for a specific deployment.
ISO/IEC TR 20226:2025 Published • environmental sustainability	Overview of environmental sustainability aspects of AI systems.	A universal environmental acceptability threshold or a verified footprint.

B6 IEEE standards and human consequences

Instrument and status	What it contributes	What it does not establish by itself
IEEE 7000-2021 Active • ethical design processes	Integrates stakeholder values into system design with traceability. Also adopted as ISO/IEC/IEEE 24748-7000:2022.	Agreement on all ethical trade-offs or proof that every outcome is ethically acceptable.
IEEE 7001-2021 Active • transparency	Measurable levels of transparency for autonomous systems.	Correctness, fairness or safety merely from transparency.
IEEE 7002-2022 Published • privacy process	Systems/software engineering requirements for privacy considerations.	Compliance with every privacy law or lawfulness of a particular use.
IEEE 7003-2024 Active • algorithmic bias	Processes addressing bias, validation datasets, application boundaries and interpretation. Published January 2025.	A universal fairness metric or adequate validation outside the assessed boundaries.
IEEE 7005-2021 Published • employee data governance	Methods for handling employee data through its life cycle.	That workplace monitoring is necessary, proportionate or lawful in a given jurisdiction.
IEEE 7009-2024 Published • fail-safe design	Technical approaches for fail-safe mechanisms in autonomous and semi-autonomous systems.	That every failure has a safe state or that a safety case is complete.
IEEE 7010-2020 Published • recommended practice	Assessment of effects of autonomous/intelligent systems on human well-being.	An agreed universal trade-off between organizational benefit and harm to others.
IEEE 7014-2024 Active • emulated empathy	Ethical considerations for systems that emulate aspects of human empathy.	That simulated empathy reflects understanding or is appropriate in every relationship.

B7 Frameworks principles and resources

Instrument and status	What it contributes	What it does not establish by itself
NIST AI RMF 1.0 / AI 100-1 Published 2023 • voluntary framework; revision underway	Organizes AI risk work through Govern, Map, Measure and Manage.	A NIST certification, fixed risk tolerances or an automatic compliance determination.
NIST AI 600-1 Published 2024 • generative-AI profile	Companion to AI RMF identifying generative-AI risks and suggested actions.	A standalone management system or proof that applying suggested actions eliminated risk.
OECD AI Principles Adopted 2019 • updated 2024	Intergovernmental principles and policy recommendations supporting trustworthy AI.	A technical test suite or an organizational certification standard.
UNESCO Recommendation on AI Ethics Adopted 2021 • normative recommendation	Human-rights, dignity, social and environmental foundation for responsible AI.	A product certificate or a replacement for domestic legal obligations.
OWASP LLM Top 10 2026 Published • community security guidance	Threat categories, attack scenarios and mitigations for LLM applications; supersedes the 2025 list.	A complete enterprise risk register or an exhaustive security test.
OWASP Top 10 for Agentic Applications 2026 Published • community security guidance	Agent-specific security risks and mitigations.	All governance needs of autonomous systems or certification of an agent.
OWASP Agent Control Standard Community specification • version 0.1.0 • listed September 2026	Defines hooks and runtime control contracts for AI agents. The linked project includes schemas and reference implementation material.	An early community specification does not establish broad interoperability, effective deployed policy or conformity to an ISO/IEC standard.
MITRE ATLAS Living knowledge base	Adversary tactics, techniques and cases involving AI.	An exhaustive account of attacks or a management-system certificate.
C2PA Technical Specification 2.4 Published technical specification • version 2.4	Technical structure for signed content provenance and validation of associated claims.	Truth of depicted events, completeness of provenance or factual accuracy of generated claims.

B8 Regional and national approaches

Instrument and status	What it contributes	What it does not establish by itself
EN 18286:2026 Published • cited in OJEU 14 October 2026	Quality management standard for EU AI Act regulatory purposes. Its reference was published through Implementing Decision (EU) 2026/2274 on 14 October 2026.	Presumption of conformity applies only to the AI Act requirements covered by the standard or relevant parts. It is not general approval of every system or every AI Act obligation.
EN ISO/IEC 42001:2026 Published • European adoption	European adoption of ISO/IEC 42001:2023; distinguish adoption year from underlying ISO edition.	EU AI Act harmonisation merely from the EN prefix.
UK AI Cyber Security Code of Practice Published January 2025 • voluntary code	Supply-chain cybersecurity expectations and implementation guidance; informed ETSI work.	General AI governance coverage or a statutory product approval.
Singapore MGF for Generative AI Published 2024 • governance framework	Nine dimensions of governance for the generative-AI ecosystem.	An international certification standard or proof of implementation.
Singapore MGF for Agentic AI Launched January 2026 • updated May 2026	Structured governance of agentic-AI risks and emerging practices.	A universal technical specification or a certificate of safe agency.
AI Verify testing framework Published • testing framework	Assessment against AI governance principles using technical tests and process checks.	Complete coverage of every risk or legal compliance simply from running tests.
CAN/DGSI 101:2025 Published • 2025 edition designation	Ethical Design and Use of Artificial Intelligence by Small and Medium Organizations. Requirements for ethical AI design and use within the standard's organizational scope.	A worldwide legal safe harbour or universal product validation.
GB/T 45654-2025 Current • effective 1 November 2025	Chinese national standard for basic security requirements for generative-AI services.	An interchangeable equivalent of ISO governance standards or global legal approval.

B9 Safety sector validation and auditing

Instrument and status	What it contributes	What it does not establish by itself
ISO/IEC TR 5469:2024 Published • functional-safety report	Addresses AI in safety functions, safeguards around AI-controlled equipment, and AI used in safety design.	A complete functional-safety certification or all sector-specific safety requirements.
ISO/PAS 8800:2024 Published • road-vehicle AI safety	Safety-related AI in series-production road vehicles and evidence supporting safety assurance.	A generic enterprise governance standard; its scope excludes development of off-vehicle AI elements.
ANSI/UL 4600, edition 3 Active • published 17 March 2023	Safety-case framework for autonomous products; 2026 CSDS items are proposals, not a new published edition.	An all-purpose AI management system or a guarantee of zero risk.
BS 30440:2023 Current • healthcare specification	Auditable validation requirements addressing AI performance, clinical benefits and integration in healthcare.	Regulatory approval or a substitute for clinical evidence specific to the intended use.
ISO 19011:2026 Published May 2026 • edition 4	Management-system auditing guidance, audit programs and auditor competence. Replaces 2018 edition.	AI product certification or specialist technical competence from generic audit competence alone.

B10 Standards in development

Project and status at reference date	Planned topic	Publication boundary
ISO/IEC FDIS 27091 FDIS • stage 50.00	AI privacy protection	Publication or final requirements must not be assumed.
ISO/IEC 42105 Stage 60.00 • under publication since 22 October 2026	Human oversight	Publication or final requirements must not be assumed.
ISO/IEC 24970 Stage 60.00 • under publication since 24 October 2026	AI logging	Publication or final requirements must not be assumed.
ISO/IEC TS 22443 Stage 60.00 • under publication since 22 October 2026	Societal and ethical guidance	Publication or final requirements must not be assumed.
ISO/IEC TS 42119-3 Stage 60.00 • under publication since 25 September 2026	Verification and validation	Publication or final requirements must not be assumed.
ISO/IEC FDIS 25059 FDIS	Revised quality models	Publication or final requirements must not be assumed.
ISO/IEC DIS 42007 DIS	Conformity-assessment schemes	Publication or final requirements must not be assumed.

B10 Standards in development — Continued

Project and status at reference date	Planned topic	Publication boundary
ISO/IEC AWI 42003 AWI	42001 implementation	Publication or final requirements must not be assumed.
ISO/IEC DTS 25568 DTS • stage 50.00 since 29 September 2026	Generative-AI risk guidance	Publication or final requirements must not be assumed.
ISO/IEC FDIS 24029-3 FDIS	Statistical robustness methods	Publication or final requirements must not be assumed.
ISO/IEC DIS 42102 DIS	Capabilities framework	Publication or final requirements must not be assumed.
ISO/IEC DIS 4213 DIS • stage 40.60 • ballot closed 21 October 2026	Performance measurement for classification, regression, clustering and recommendation tasks. The revision is an International Standard project.	Publication or final requirements must not be assumed.
ISO/IEC CD TS 22440 parts 1 to 3 Technical Specification projects • committee drafts	Functional-safety guidance for AI systems and application examples; Part 3 is at stage 30.60.	Publication or final requirements must not be assumed.
NIST IR 8596 Initial preliminary draft	Cyber AI Profile	Publication or final requirements must not be assumed.

Pipeline status is a snapshot at 24 October 2026. Stage 60.00 means under publication, not publication completed. Generative-AI amendments to ISO/IEC 22989 and 23053 remain final draft amendments. European standardization continues through CEN-CENELEC JTC 21. A project's existence, a European adoption and an Official Journal citation are different states; none should be inferred from the others.

Status sources: [SC 42 catalogue](#)

[European Commission harmonised-standards list](#)

Choosing evidence for the decision

Coverage is a portfolio decision

AI risks form a spectrum. Security compromise is one mechanism; a harmful outcome can also arise from an inaccurate output, a valid prediction used for an unsuitable purpose, an unfair allocation of opportunity, excessive surveillance, misplaced reliance, or an organizational decision to give a system more authority than its evidence supports. A secure system can contribute to any of these outcomes without being attacked.

Different documents address parts of that spectrum. Their presence does not mean the remaining parts are ungoverned; it means the organization must identify which documents, laws, controls and evidence apply to its own use context. Treating every gap as a defect in a narrowly scoped standard would be as misleading as claiming that the standard covers everything.

Assurance question	Evidence to examine	What this alone does not establish
Authority Governing body / accountable owner	Who may authorize this use, under which constraints?	A policy title or committee alone is insufficient.
Management AIMS and operational processes	How are responsibilities, changes, suppliers and exceptions managed?	Process conformity does not establish every output's validity.
Evidence Technical and contextual evaluation	What demonstrates fitness for the task, population and operating conditions?	A supplier benchmark does not validate every downstream workflow.
Impact Affected people and objectives	Who benefits, who may be harmed, and what challenge or remedy exists?	Completing an assessment does not itself make impacts acceptable.
Security Threats and protective measures	What can be attacked, manipulated, stolen or misused?	Protection against attacks cannot settle every question of appropriate use.
Reassessment Change and operational monitoring	Which changes invalidate earlier evidence or authorization?	An assessment has an evidential boundary in time and context.

A hiring decision as a worked example

Consider a hypothetical AI tool that ranks applicants. An AIMS can structure accountability and change control. Security measures can protect the model and applicant data. Bias and testing methods can examine particular failure modes. Impact assessment can examine consequences for applicants. None of these, taken alone, demonstrates that the ranking criteria are job-relevant, that the chosen error rates are acceptable, or that a recruiter can meaningfully challenge a recommendation under real workload conditions. Those questions require evidence and judgment about the deployment.

This is an illustrative synthesis, not a finding about an actual product. It shows why the same evidence cannot be used indiscriminately for management, security, performance and social acceptability claims.