Current AI Frameworks Overview
Date: 25 January 2026

The following profiles provide essential operational context for each framework, organized by legal force (mandatory versus voluntary), and geographic scope.

Please note that the following overviews are generalized and do not include domain specific obligations or policy directives such as in healthcare, national directives, defense, or financial systems.

Determining applicability for specific use cases requires contextual analysis beyond the scope of this overview. Readers are responsible for determining relevance to their own regulatory environments.

1. EU AI Act

a. Status: Legally binding regulation in force since 1 August 2024. Phased implementation through 2027.
b. Geographic Scope
    i. All 27 EU member states
    ii. Extraterritorial application non-EU providers whose AI systems are used within the EU.
c. Core Philosophy
    i. Risk-based, horizontal framework
    ii. Prohibits unacceptable AI practices
    iii. Strict requirements for high-risk AI systems
    iv. Lighter obligations for limited-risk and minimal-risk systems
d. Key Obligations
    i. Risk management systems
    ii. Data governance and quality requirements
    iii. Technical documentation
    iv. Human oversight mechanisms
    v. Transparency and disclosure
    vi. Conformity assessments
    vii. Post-market monitoring
e. Primary Audience
    i. Providers, deployers, importers, and distributors of AI systems
    ii. Mandatory for high-risk systems in:

1. Healthcare
2. Critical infrastructure
3. Law
4. Employment
5. Education
6. Financial systems

f. Implementation Timeline
   i. 2 February 2025 – Prohibited practices and AI Literacy
   ii. 2 August 2025 – GPAI (General-Purpose Artificial Intelligence) obligations and governance
   iii. 2 August 2026 – High-risk systems requirements (Annex III)
   iv. 2 August 2027 – Product embedded high-risk systems
   v. 31 December 2030 – Large-scale IT systems compliance

g. Penalties/Enforcement
   i. Up to €35 million or 7% of global annual turnover for prohibited practices
   ii. Up to €15 million or 3% of global annual turnover for non-compliance with other obligations
   iii. Up to €7.5 million or 1% of global annual turnover for incorrect information supplied to authorities
      1. Note: Under Article 99(5) – Offenses – it is NOT specified whether supplied information is intentional or unintentional, only that the data is misrepresented.
         a. ***"The supply of incorrect, incomplete or misleading information to notified bodies or national competent authorities in reply to a request shall be subject to administrative fines of up to €7,500,000 or, if the offender is an undertaking, up to 1% of its total worldwide annual turnover for the preceding financial year, whichever is higher."***
      2. Note: Under Article 99(7) – Penalties – it IS specified that penalties will be imposed upon consideration of intent.
         a. ***"When deciding on the amount of the administrative fine in each individual case, all relevant circumstances of the specific situation shall be taken into account… (i) the intentional or negligent character of the infringement…"***

h. Notable Features

i. First comprehensive, legally binding AI regulation globally.
ii. Established EU AI Office for enforcement.
iii. Code of Practice for GPAI models published August 2025.
iv. Digital Omnibus Package published November 2025 and proposes simplification measures.

2. NIST AI Risk Management Framework

a. Status: Voluntary framework released January 2023
    i. NIST RMF is increasingly being adopted as the de facto standard and is frequently referenced in legislation.
b. Geographic Scope
    i. United States federal government recommended standard.
    ii. Global application: voluntary in the private sector worldwide.
c. Core Philosophy
    i. Risk-based
    ii. Trustworthiness focused: emphasizes characteristics of trustworthy AI
        1. Valid/reliable
        2. Safe
        3. Secure/resilient
        4. Accountable/Transparent
        5. Explainable/interpretable
        6. Privacy-enhanced
        7. Fair and unbiased
        8. Technology agnostic and sector-neutral
d. Key Obligations
    i. Govern: establish governance structures and policies
    ii. Map: Understand AI systems context and risk
    iii. Measure: Assess AI systems performance and impact
    iv. Manage: Prioritize and respond to identified risks
e. Primary Audience
    i. Federal Agencies
    ii. Private sector organizations developing/deploying AI systems
    iii. International organizations seeking alignment with U.S. standards
f. Implementation Timeline
    i. Voluntary framework - no mandatory timelines released
    ii. Cybersecurity Framework Profile for AI preliminary draft released December 2025

iii. Initial Public draft expected 2026

g. Penalties/Enforcement
    i. None – NIST RMF is a voluntary framework
    ii. However, NIST RMF is increasingly becoming referenced in contracts, procurement requirements, and as affirmative defense in litigation (e.g., TRAIGA).
h. Notable Features
    i. Most widely adopted voluntary AI framework globally.
    ii. Developed through transparent, consensus-driven process with extensive stakeholder input.
    iii. Companion resources include Playbook, Crosswalks to other frameworks, and sector-specific profiles.

3. ISO/IEC 42001

a. Status: Voluntary international certification standard published in December 2023; first certifiable management system standard specifically for AI.
b. Geographic Scope
    i. Global
    ii. Published by ISO and IEC – internationally recognized standardization body.
c. Core Philosophy
    i. Management systems approach on ISO 9001 (quality) and ISO 27001 (information security).
    ii. Focuses on establishing, implementing, maintaining, and continually improving an AI management system.
d. Key Obligations
    i. Context understanding and stakeholder engagement
    ii. Leadership and governance structures
    iii. AI policy and objectives
    iv. Risk assessment and treatment
    v. Resource Management
    vi. Operational Controls
    vii. Performance Evaluation
    viii. Continual Improvement
e. Primary Audience
    i. Organizations seeking third-party certification of AI management practices

ii. Companies with existing ISO management systems (27001, 9001) extending certification to AI practices
iii. Enterprises demonstrating AI governance maturity to customers/regulators

f. Implementation Timeline
    i. Voluntary framework - no mandatory timelines released
    ii. Organizations pursue certification when prepared.
    iii. Certification bodies accredited to audit against standard.
g. Penalties/Enforcement
    i. None – ISO/IEC 42001 is a voluntary framework
    ii. Non-compliance can result in certification suspension/withdrawal but no legal penalties.
h. Notable Features
    i. Integrates with ISO management systems.
    ii. Certification demonstrates third-party validated AI governance.
    iii. Emphasizes documented processes, records, and continuous improvement cycles.

4. OECD AI Principles

a. Status: Non-binding principles adopted May 2019 and updated in 2024; 47 member countries plus additional adherents.
    i. Forms the conceptual basis for many national AI policies.
b. Geographic Scope
    i. Global
    ii. OECD countries include most economically advanced countries: U.S., EU countries, Japan, South Korea, Canada, Australia, etc.
    iii. Organizations located outside of these geographic jurisdictions can voluntarily adhere.
c. Core Philosophy
    i. Principles-based approach emphasizing values and human-centric design.
    ii. Five principles:
        1. Inclusive growth/Sustainable development/well-being
        2. Human-centered values/fairness
        3. Transparency/explainability
        4. Robustness/security/safety
        5. Accountability
d. Key Obligations

i. Recommendations for policy-makers – not binding mandates
ii. Invest in AI R&D
iii. Foster digital ecosystems
iv. Shape enabling policy environment
v. Build human capacity
vi. International cooperation

e. Primary Audience
    i. National governments developing AI strategies and policies
    ii. International organizations coordinating AI governance
    iii. Private sector as guidance
f. Implementation Timeline
    i. Voluntary framework – no mandatory timelines released
    ii. Member countries are expected to align national policies with principles over time
g. Penalties/Enforcement
    i. None – OECD AI Principles is a voluntary framework
    ii. This is a soft law instrument that influences through diplomatic and reputational mechanisms.
h. Notable Features
    i. First international consensus on AI governance principles.
    ii. Foundation for GPAI.
    iii. Influenced development of the EU AI Act, Council of Europe Treaty, and many national frameworks.

5. White House AI Bill of Rights

a. Status: A non-binding policy document published October 2022
    i. This document represents the U.S. Administration's position but is not legally enforceable
b. Geographic Scope
    i. United States
    ii. Document represents federal policy guidance
    iii. No legal force but influences federal procurement and agency rulemaking
c. Core Philosophy
    i. Individual rights centric
    ii. Five principles:
        1. Safe/effective systems
        2. Algorithmic discrimination protections

3. Data privacy
4. Notice and explanation
5. Human alternatives/consideration/fallback

d. Key Obligations
    i. Recommendations only
    ii. Conduct impact assessments
    iii. Provide transparency of use of automated systems
    iv. Enable meaningful human review
    v. Protect against discriminatory outcomes
    vi. Respect data privacy
e. Primary Audience
    i. Federal agencies developing automated systems
    ii. Technology developers seeking to align with federal expectations
    iii. Civil society organizations advocating for protections against AI biases and unfairness.
f. Implementation Timeline
    i. Voluntary framework – no mandatory timelines released
    ii. Some provisions incorporated into agency-specific rules (EEOC AI and employment guidance).
g. Penalties/Enforcement
    i. None – White House AI Bill of Rights is a voluntary framework
    ii. Soft law with influence through federal procurement requirements and agency policy adoption
h. Notable Features
    i. Individual rights-focused rather than risk-based framework.
    ii. Strong emphasis on algorithmic discrimination and civil rights.
    iii. Influenced state-level AI legislation including parts of individual state policies (e.g., Colorado AI Act).

6. TRAIGA (Texas Responsible AI Governance Act)

a. Status: State legislation signed 22 June 2025 and becomes enforceable 1 January 2026.
    i. Makes Texas the second state after Colorado to enact comprehensive AI legislation.
b. Geographic Scope
    i. State of Texas, United States

ii. Applies to any individual/entity conducting business in Texas, offering products/services to Texas residents, or developing/deploying AI in Texas.

c. Core Philosophy
    i. Intent-based liability model
    ii. Heavily geared toward regulations for governmental entities with soft, implied requirements in the private sector
    iii. Prohibits specific harmful AI practices rather than broad risk-based assessments.
    iv. More business-friendly than original proposal that mirrored the EU AI Act.
d. Key Obligations
    i. Prohibited uses (governmental and private sectors):
        1. Intentional discrimination
        2. Behavioral manipulation for harm
        3. Impairment of constitutional rights
        4. Production of illegal content (CSAM, unlawful deepfakes)
    ii. Prohibited uses (governmental):
        1. Use of AI systems for social scoring
        2. Use of AI for biometric identification without consent
e. Primary Audience
    i. Private sector developers and deployers in Texas
    ii. Government agencies using AI systems
    iii. Healthcare providers using AI systems for diagnosis and treatment
    iv. Financial institutions
f. Implementation Timeline
    i. 1 January 2026 – Full enforcement begins.
    ii. Regulatory sandbox applications open with a 36 month program.
        1. Official Project Name: AI Regulatory Sandbox Program
        2. Administrator: Texas Department of Information Resources (DIR) + Texas AI Advisory Council
        3. Purpose: A controlled testing environment that allows companies to test innovative AI systems without obtaining standard state licenses, registrations, or regulatory authorizations that would normally be required.
        4. Legal Protections:
            a. Texas Attorney General cannot file charges for violations of waived laws/regulations.

b. State agencies cannot pursue punitive action for waived violations.
c. Provides protection from penalties and enforcement for experimental systems with proper application and approval

g. Penalties/Enforcement
    i. Enforcement and penalties occur through the Texas Attorney General.
    ii. 60 day buffer period for violations.
    iii. **$10,000 - $12,000 per curable offense.**
        1. Process for a "curable" offense:
            a. Texas AG sends notice of violation.
            b. Company receives 60 days to fix the problem.
            c. Company submits documentation proving they have fixed the violation.
        2. If the offense has been fixed within this time period, it results in lower penalties or possibly no enforcement action, as deemed appropriate by Texas AG.
        3. $2,000 – 40,000 fee per day for continuing violations.
    iv. **$80,000 – 200,000 per uncurable violation.**
        1. A violation is deemed uncurable if it cannot be undone or if the harm is irreversible.
        2. No buffer period applies – penalties apply immediately once court has determined violation
        3. Examples:
            a. AI system deployed with intent to discriminated against protected groups and it is proven that 50 people have already been denied jobs.
            b. AI systems intentionally incited self-harm; the person is proven to already have been harmed.
            c. AI systems were used to intentionally created CSAM or deepfake media; these exist and have been distributed.
    v. No private right of action
        1. Individuals and private parties cannot sue for TRAIGA violations and offenses: these must come through the Texas Attorney General.
h. Notable Features
    i. Intent-based rather than impact-based liabilities.

ii. Substantial and documented compliance with NIST AI RMF serves as affirmative defense against TRAIGA violations.
iii. Establishes Texas AI Advisory Council.
iv. Establishes Regulatory Sandbox Program for innovation.
v. Pending federal preemption concerns
    1. 10-year moratorium proposed but ultimately stripped from bill in July 2025.

7. Council of Europe AI Treaty

a. Status: First legally binding international AI Treaty adopted on 17 May 2024 and opened for signature on 5 September 2024.
b. Geographic Scope
    i. Council of Europe members – 46 countries including all EU members.
    ii. Open to non-member states globally.
    iii. Signed by EU, U.S., Canada, Japan, Switzerland, etc.
c. Core Philosophy
    i. Human rights, democracy, and rule of law approach
    ii. Technology neutral
    iii. Focuses on AI lifecycle activities rather than specific technologies
    iv. Balances innovation with fundamental human rights protections
d. Key Obligations
    i. Risk and impact assessments
    ii. Transparency and explainability
    iii. Human rights safeguards
    iv. Right to challenge AI-driven decisions
    v. Prohibition of AI practices violating human rights
    vi. Procedural remedies for rights violations
    vii. Continuous monitoring throughout AI lifecycle
e. Primary Audience
    i. Public authorities in signatory states
    ii. Private entities acting on behalf of public authorities
    iii. Private sector parties that choose direct application or alternative compliance measures
f. Implementation Timeline
    i. 1 November 2025 – Enforcement begins
    ii. Each member state determines national implementation schedule.
    iii. Flexible provisions allow parties to exclude national security and national defense initiatives.

g. Penalties/Enforcement
    i. Enforcement determined by each member state.
    ii. Conference of the Parties oversees implementation.
    iii. European Court of Human Rights may incorporate treaty into jurisprudence.
h. Notable Features
    i. First globally binding AI Treaty (not limited to Europe)
    ii. Complements EU AI Act but focuses on human rights rather than market regulation
    iii. Allows flexible implementation – direct obligation or alternative measures
    iv. National defense and R&D generally excluded from provisions

8. Singapore AI Verify

a. Status: Voluntary testing framework and toolkit initially released in 2022 for traditional AI systems
    i. Updated in May 2025 to address generative AI systems
    ii. Part of a broader AI governance ecosystem including the Model AI Governance Framework
b. Geographic Scope
    i. Singapore (national framework)
    ii. Global influence through AI Verify Foundation (an open-source community)
        1. AI Verify Foundation – Collaborative development with 70+ global organizations including OpenAI, Google, Microsoft, and Anthropic.
c. Core Philosophy
    i. Testing and assurance approach.
    ii. Validates AI system performance against 11 internationally recognized principles through standardized tests.
    iii. Combines technical testing with process checks.
    iv. Emphasis on transparency and trust-building.
d. Key Obligations
    i. Voluntary testing against 11 principles:
        1. Transparency
        2. Explainability
        3. Repeatability/Reproducibility
        4. Safety/Robustness

5. Fairness
6. Data governance
7. Accountability
8. Human-agency/oversight
9. Secure-by-design
10. Inclusive growth
11. Environmental sustainability

e. Primary Audience
    i. AI system developers and deployers in Singapore and globally
    ii. Organizations demonstrating responsible AI to customers/regulators
    iii. Companies participating in Global AI Assurance Sandbox
        1. Official Project Name: Global AI Assurance Sandbox (also called Generative AI Evaluation Sandbox)
        2. Administrator: IMDA (Infocomm Media Development Authority) + AI Verify Foundation
        3. Launch Date: July 2025
f. Implementation Timeline
    i. Ongoing evolution
    ii. Model Framework – published 2019; updated 2020
    iii. AI Verify Toolkit – 2022
    iv. AI Verify Foundation – 2023
    v. Generative AI Framework – 2024
    vi. Generative AI updates to AI Verify – May 2025
    vii. Model AI Governance Framework for Agentic AI (January 2026)
g. Penalties/Enforcement
    i. None – Singapore AI Verify is a voluntary framework
    ii. Singapore's AI Safety Institute (established 2025) provides guidance.
    iii. No legal mandate but the framework is becoming increasingly embedded into procurement standards.
h. Notable Features
    i. World's first AI governance testing framework combining technical tests with process validation.
    ii. Open-source through AI Verify Foundation.
    iii. Global AI Assurance Pilot codifying best practices for AI use.
    iv. Singapore AI Safety Red-Teaming Challenge (2024-2025) focused on multicultural/multilingual safety measures.
    v. Project Moonshot: open-source LLM evaluation toolkit for red-teaming.

Quick Overlap Analysis

The following requirements appear consistently across all eight frameworks, representing the core foundation of known AI Governance:

1. Risk Management: All frameworks require or strongly recommend systemic identification, assessment, and mitigation of AI-related risks.
2. Accountability: Clear assignment of roles and responsibilities for AI system decisions and outcomes.
3. Transparency: Disclosure of AI system use, capabilities, and limitations to appropriate stakeholders.
4. Human Agency: Preservation of meaningful human control over consequential AI decisions.
5. Fairness Principles: Prevention of discriminatory outcomes and data-based biases in AI systems.
6. Safety and Security: Protection against AI system failures, attacks, and unintended consequences.
7. Lifecycle Governance: Continuous oversight from design through deployment to decommissioning.
8. Documentation: Maintenance of records sufficient to demonstrate governance compliance.

Strong Correlations

The following requirements appear in most frameworks, indicating strong international consensus:

1. Data Quality Requirements: Standards for training data representativeness, accuracy, and relevance to system applications.
2. Impact Assessments: Evaluation of potential societal, ethical, and rights implications.
3. Explainability: Ability to provide meaningful explanations of AI systems decisions.
4. Continuous Monitoring: Post-deployment/Post-market surveillance of AI system performance metrics.
5. Stakeholder Engagement: Consideration of affected parties in AI system design and deployment.
6. Third-Party Assessment: Independent validation of AI system compliance or performance.

Notable Quantitative Overlap Assessments

1. At least ~60% of these core requirements overlap across frameworks when mapped to governance categories.
2. This overlap increases to ~80% considering “principles” convergence rather than implementation specific requirements.

Conclusion

A single, well-designed governance system can satisfy multiple frameworks simultaneously by addressing common requirements while maintaining flexibility or framework-specific nuances. This degree of convergence supports a stacked governance architecture, a common core that satisfies shared obligations with modular extensions for framework- and domain-specific requirements.