Global AI governance in 2026: A seven-jurisdiction board briefing

AI governance is imperative for directors

May 2026

Executive summary

AI has become a board-level governance obligation. Organizations are adopting AI far faster than they can govern it. A 2025 survey by the National Association of Corporate Directors (NACD) reveals that while 62% of boards now hold regular AI discussions, only 27% have formally added AI governance to their committee charters.[1]

The regulatory landscape has shifted decisively. The EU AI Act took effect on 1 August 2024 and all sections will fully apply on 2 August 2026. On 20 March 2026, the White House released a National Policy Framework for Artificial Intelligence, outlining policy recommendations to guide Congress in developing a unified federal approach to AI legislation. China has written AI governance into foundational national law. India, Singapore and Australia are each pursuing distinct but converging strategies. The UK is anticipated to introduce formal legislation in the second half of 2026.[2]

For directors, the message is clear: AI governance is now a fiduciary matter, not a technology project.

This guide maps the regulatory landscape of seven jurisdictions, quantifies the risks of inaction and provides a practical framework for boards to follow.

[1]National Association of Corporate Directors. Data Pack: Artificial Intelligence, 2025 Public Company Board Practices Oversight Survey.

[2]Alla Valente. AI regulations clear major hurdles on both sides of the Atlantic. Forrester. 23 July 2025;
European Commission. AI Act enters into force. Accessed in April 2026;
EU Artificial Intelligence. Implementation timeline. Accessed in April 2026;
The White House. President Donald J. Trump unveils national AI legislative framework. 20 March 2026.
Library of Congress. China: Amended cybersecurity law takes effect. Accessed in April 2026;
GSMA. Member Briefing: The emerging AI policy landscape, Asia-Pacific. Accessed in April 2026;
Aninda Chakraborty. UK defers AI regulation bill for detailed future legislation. Tech Monitor. 09 June 2025.

Contents

Why AI governance is a board-level matter

The disconnect between AI adoption and board preparedness is substantial.

The governance gap

While "40% of organizations urgently remain in the developing or formalizing governance stages, only 10% have a dedicated AI governance team and fewer than half have even basic AI usage policies."[3] Just 27% of boards have formally incorporated AI governance into committee charters.

A 2026 Cisco report states that "Only 12% of organizations describe their AI governance committee as mature and proactive."[4]

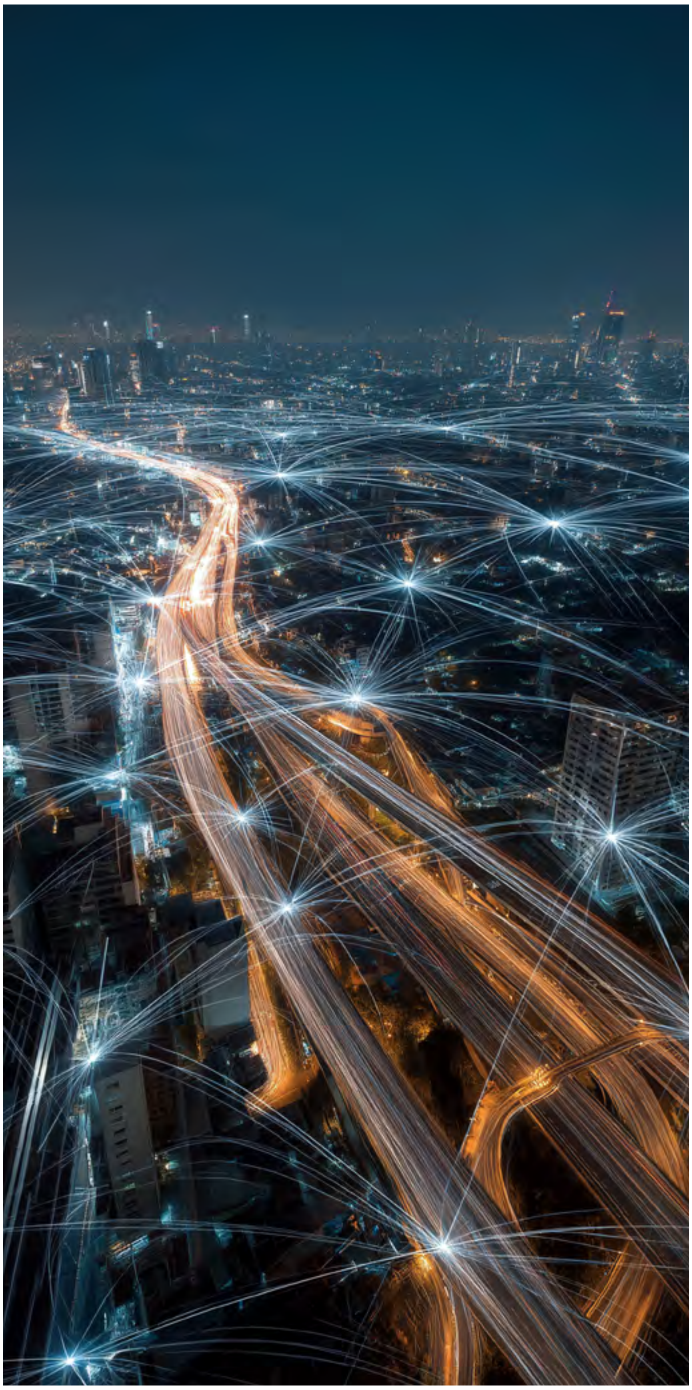
The business case for board-level AI governance

70% of Fortune 500 executives surveyed say their companies have AI risk committees, 67% report progress on AI infrastructure and 41% have a dedicated AI governance team. Yet only 14% say they are fully ready for AI deployment, underscoring a growing gap between formal governance structures and real-world AI readiness.[5]

Governance is not bureaucratic overhead — it's the mechanism that differentiates value creation from value destruction. Research shows that centralized AI governance is a key characteristic of AI leaders. They achieve a significantly higher ROI compared to AI laggards.[6]

The market opportunity

"The global AI governance market size was valued at $308.3 million in 2025 and is projected to reach $3,590.2 million by 2033, growing at a compound annual growth rate (CAGR) of 36.0% from 2026 to 2033. The healthcare and life sciences segment is expected to grow at the fastest CAGR of 39.9% from 2026 to 2033."[7] This rapid growth signals that AI governance is an emerging strategic investment.



[3]Optro. The AI oversight gap. 2025.

[4]Cisco. A Shifting Paradigm: Governance in the Age of AI. Cisco 2026 Data and Privacy Benchmark Study. 2026.

[5]sedgwick. 2026 Global Risk Study. Accessed in April 2026.

[6]NTT DATA. 2026 Global AI Report: A Playbook for AI Leaders.

[7]Grand View Research. AI Governance Market (2026 - 2033). Market analysis report.

The regulatory landscape: An overview of seven jurisdictions

1. European Union (EU): EU AI Act

Element	Detail
Instrument	Regulation (EU) 2024/1689 — Artificial Intelligence Act
Enacted	Published 12 July 2024; came into force 1 August 2024
Full application	2 August 2026 (majority of provisions)
Source	eur-lex.europa.eu

The AI Act came into force on 1 August 2024 with full applicability on 2 August 2026, with exceptions:

- The regulations on prohibited AI practices and AI literacy obligations took effect on 2 February 2025.
- The governance rules and obligations for general-purpose AI (GPAI) models became applicable on 2 August 2025.
- The rules for high-risk AI systems embedded in regulated products carry an extended transition window ending on 2 December 2027 for standalone high-risk AI systems and 2 August 2028 for high-risk embedded in products.

The AI Digital Omnibus complication

The Digital Omnibus (introduced by the European Commission in November 2025) is a legislative package intended to align EU digital laws to reduce regulatory burden and improve implementation.[8]

Over the course of 2025, it became increasingly clear that the publication of key guidance, standards and other relevant documentation would be delayed, leaving little to no time for organizations to prepare for the compliance deadline of 2 August 2026. Media reports indicate that the European Parliament aims to undertake trilogue talks in April or early May 2026; it's unknown how long negotiations will take.[9] Until the AI Digital Omnibus is enacted, the deadline for compliance with Annex III: High-risk AI systems remains 2 August 2026 for the majority of rules and 2 August 2027 for high-risk AI embedded in regulated products.

Penalty structure[10]

Tier	Maximum fine*
Prohibited AI practices	Up to €35 million or up to 7% of global annual turnover
High-risk system obligations	Up to €15 million or up to 3% of global annual turnover
Misleading information to authorities	Up to €7.5 million or 1% of global annual turnover

*whichever is higher

Board implications and actions

Until 2 August 2026, boards should ensure all AI systems are classified, assessing whether they fall under high-risk or prohibited categories, and implement relevant measures for risk management, human oversight, data governance and transparency.

By 2 August 2026, conformity assessments should be completed, technical documentation finalized and EU database registration for high-risk systems completed.

[8]European Union. Digital Omnibus Regulation Proposal. Accessed in April 2026.

[9]Jennifer Rankin. European Commission accused of 'massive rollback' of digital protections. The Guardian. 19 November 2025; Supantha Mukherjee and Bart H. Meijer. EU to delay 'high risk' AI rules until 2027 after Big Tech pushback. Investing.com. 19 November 2025.

[10]European Union. EU Artificial Intelligence Act, Article 99: Penalties. Accessed in April 2026.

2. US: Federal deregulation and state fragmentation

Element	Detail
Current federal instruments	Executive Order (EO) 14179 (January 2025) EO 14365 (December 2025) National Policy Framework for Artificial Intelligence (20 March 2026)
Key standards	National Institute of Standards and Technology (NIST) AI Risk Management Framework (AI RMF) 1.0
State activity	50 states and territories introduced AI legislation in 2025; 38 states adopted approximately 100 measures
Sources	whitehouse.gov; nist.gov

On 20 March 2026, the White House released a National Policy Framework for Artificial Intelligence, outlining policy recommendations to guide Congress. The policy recommendations signal that the proliferation of state AI laws is creating barriers to innovation, that there needs to be some national standard governing AI and that Congress should act to protect individuals from potential harm.

The US does not have a single comprehensive federal law regulating AI. Federal AI governance currently relies on agency enforcement under existing laws, executive orders and voluntary guidelines.

State-level activity

In 2025 alone, all 50 states, Washington DC, Puerto Rico and the US Virgin Islands introduced AI-related legislation, with 38 states adopting or enacting such laws. Key enactments effective in 2026 include:

- California's Transparency in Frontier Artificial Intelligence Act and Texas's Responsible Artificial Intelligence Governance Act are two prominent examples of state AI laws that took effect on 1 January 2026
- Colorado AI Act (SB24-205): Operational requirements are effective from June 2026

The federal–state tension

For now, organizations remain subject to an uneven mix of state requirements, federal enforcement through existing authorities and political uncertainty regarding whether Congress will adopt the White House's approach or not.

Organizations should use this time to build well-documented AI governance programs that are adaptable and resilient.

3. UK and Ireland: Principles-based, awaiting legislation

Element	Detail
Current framework	Policy paper: AI regulation: a pro-innovation approach (March 2023; updated August 2023)
Five core principles	Safety and robustness; transparency; fairness, accountability; and contestability and redress
Anticipated legislation	AI bill expected second half of 2026 at the earliest
Source	gov.uk

An anticipated UK AI bill did not materialize during 2025. The UK government appears to be focusing on innovation through AI Growth Zones and AI Growth Labs (regulatory sandboxes). Whether a dedicated AI bill will appear in 2026 remains uncertain.

The UK is taking a principles-based, sector-led approach to AI regulation. Instead of enacting a single AI law like the EU AI Act, the UK currently relies on existing regulators and voluntary standards. However, as generative and frontier AI systems create new governance challenges, the momentum toward a formal statutory framework is growing.

An AI bill, expected to be proposed in the second half of 2026 at the earliest, will likely address copyright matters as well as the most powerful AI models.

Board implications and actions

Organizations operating in the UK should prepare for sector-specific regulatory scrutiny from bodies including the Information Commissioner's Office (ICO), Ofcom, Competition and Markets Authority (CMA) and Financial Conduct Authority (FCA). The absence of an AI law does not mean the absence of enforceable obligations — data protection, consumer law, equality legislation and online safety rules already apply to AI systems.

4. Australia: Regulate where necessary

Element	Detail
Key policy instrument	National AI Plan 2025 (released 2 December 2025)
Voluntary standard	Guidance for AI Adoption (AI6, October 2025)
AI Safety Institute	A$29.9 million; operational early 2026[11]
Sources	industry.gov.au; digital.gov.au

The National AI Plan seeks to boost Australia's reputation as a place in which to invest in AI. Rather than establishing mandatory guardrails for AI in high-risk settings, Australia will instead "continue to build on Australia's robust existing legal and regulatory frameworks, ensuring that established laws remain the foundation for addressing and mitigating AI-related risks."[12]

The Australian government is establishing an AI Safety Institute (AISI) to respond to AI-related risks and harms. The AISI will become operational in early 2026.

No economy-wide AI law is coming soon. The government will incrementally amend existing regulation and legislation, including the Privacy Act, the Australian Consumer Law and, possibly, the Online Safety Act.

Board implications and actions

The absence of standalone AI legislation should not be confused with the absence of enforceable obligations. The Privacy Act reforms that will introduce transparency obligations for automated decision-making take effect in December 2026. Boards must ensure AI systems comply with existing laws governing privacy, consumer protection and corporate governance, as well as with sector-specific regulations.

[11]Australian Government Department of Industry, Science and Resources. Australia to establish new institute to strengthen AI safety. 25 November 2025.

[12]AIPP. Australia unveils AI policy roadmap. 2 December 2025.

5. India: A pro-innovation, techno–legal sectoral approach

Element	Detail
Primary AI policy	India AI Governance Guidelines (Ministry of Electronics and Information Technology, 5 November 2025)
Key data protection law	Digital Personal Data Protection Act (DPDPA), 2023
Seven guiding principles ("sutras")	Trust; people first; innovation over restraint; fairness and equity; accountability; understandable by design; and safety, resilience and sustainability
Source	meity.gov.in; indiaai.gov.in

The Ministry of Electronics and Information Technology (MeitY), under the IndiaAI Mission, unveiled the India AI Governance Guidelines, a comprehensive framework for safe, inclusive and responsible AI adoption across sectors.

These guidelines advocate a "lightweight" and adaptive regulatory approach that leverages existing laws and promotes innovation with appropriate safeguards.

Core framework

The framework sets out seven sutras and six governance pillars: infrastructure, capacity building, policy and regulation, risk mitigation, accountability and institutions.

Institutional architecture

Key recommended bodies are:

- Forming an AI governance group (AIGG) as a small, permanent interagency policy body
- Gathering a technology and policy expert committee to advise on the AIGG
- Establishing an AI Safety Institute (AISI) for testing, standards and safety research.

Sectoral regulation

The Reserve Bank of India released the Framework for Responsible and Ethical Enablement of Artificial Intelligence (FREE-AI) on 13 August 2025. It addresses AI governance and risk management within the financial sector and sets out 7 guiding sutras and 26 recommendations across 6 pillars.

Board implications and actions

The DPDP Act governs the use of personal data for training AI models. This means organizations must obtain consent before using individuals' data to train AI, or risk violating data protection rules. Boards with financial services operations in India should note that the Reserve Bank of India (RBI) FREE-AI Report recommends finance-sector institutional measures, including board-approved AI policies for regulated entities, strengthening internal and third-party audit frameworks for AI, and establishing incident-reporting mechanisms.[13]

[13] Reserve Bank of India. Framework for Responsible and Ethical Enablement of Artificial Intelligence.

6. Singapore: Assurance-first voluntary-led governance hub

Element	Detail
National AI strategy	National Artificial Intelligence Strategy (NAIS) 2.0 (December 2023)
Core governance framework	Model AI Governance Framework (second ed. 2020; GenAI ed. 2024)
Agentic AI framework	Model AI Governance Framework for Agentic AI (January 2026), a world first
AI testing toolkit	AI Verify, the world's first government-developed AI governance testing framework
Data protection law	Personal Data Protection Act 2012 (PDPA), as amended in 2020
Source	imda.gov.sg; pdpc.gov.sg; mas.gov.sg

Singapore has positioned itself as a leading jurisdiction for AI governance through a deliberately pro-innovation regulatory model. Rather than adopting a single, binding AI statute, Singapore relies on a combination of national strategies, voluntary governance frameworks, sector-specific guidance and practical implementation tools. This approach reflects a policy choice to encourage responsible AI adoption while preserving flexibility.

Agentic AI, a world first

On 22 January 2026, Singapore unveiled the Model AI Governance Framework (MGF) for agentic AI at the 2026 World Economic Forum. The framework represents the world's first dedicated governance model for agentic AI systems — AI agents capable of independently reasoning, planning and executing tasks. Although the MGF does not impose binding legal obligations, it provides a strong indication of Singapore's regulatory trajectory.

AI Verify

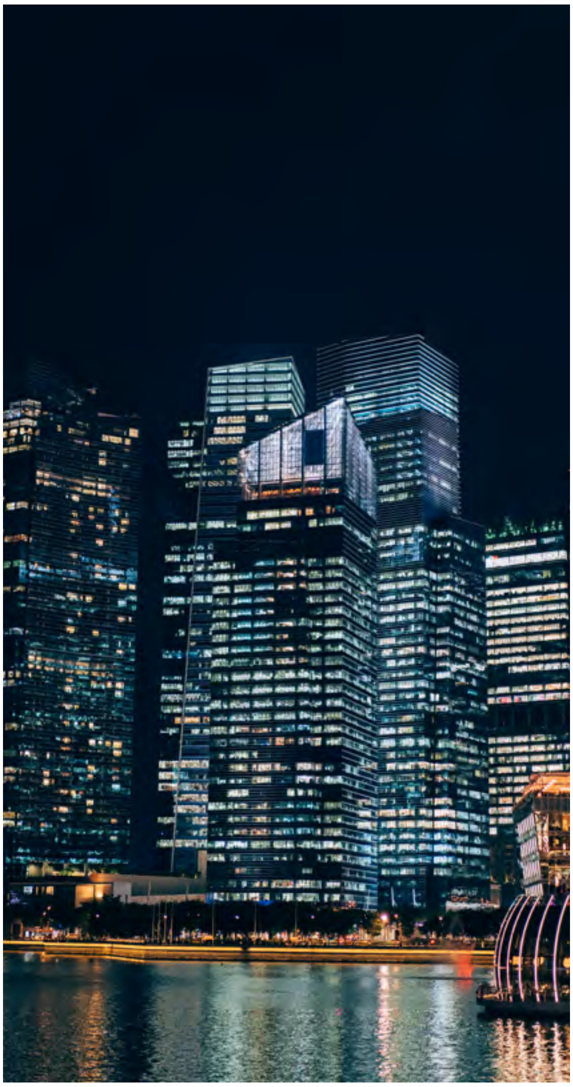
The AI Verify governance testing framework consists of 11 AI ethics principles consistent with internationally recognized AI frameworks such as those from the EU, OECD and Singapore's MGF. AI Verify helps organizations validate the performance of their AI systems against these principles through standardized tests.

National investment

NAIS 2.0 allocates more than S$1 billion over five years to advance AI capabilities, digital trust and workforce readiness.[14]

Board implications and actions

For businesses operating in or from Singapore, AI compliance is not a matter of satisfying a single legal act, but of navigating an ecosystem of interlocking frameworks and sectoral expectations. Singapore's frameworks serve as the de facto governance standard for operations from the Association of Southeast Asian Nations and are increasingly being used as a bridge for cross-border compliance with EU and US requirements.



[14]Smart Nation Singapore. National AI Strategy. Accessed in April 2026.

7. China: State-directed, layered and enforced

Element	Detail
Foundational cyber/data laws	Cybersecurity Law (CSL, 2017; amended October 2025, effective 1 January 2026) Data Security Law (DSL, 2021) Personal Information Protection Law (PIPL, 2021)
Generative AI (GenAI) regulation	Interim Measures for Administration of Generative AI Services (effective 15 August 2023)
AI content labeling	Administrative Measures for AI-Generated Content Labeling (effective 1 September 2025)
Sources	cac.gov.cn; npc.gov.cn

CSL amendments: AI enters national law

On 28 October 2025, China's central legislature approved amendments to the Cybersecurity Law, to take effect on 1 January 2026. The amendments introduce dedicated provisions for AI governance and significantly strengthen penalties for data and cybersecurity violations.

Although China has already introduced rules on algorithms, deepfake technology, GenAI and AI labeling, this marks the first time that AI governance has been formally written into one of China's foundational cybersecurity laws, elevating AI governance from regulation to legislation.

Extraterritorial enforcement

The amendments broaden the scope of activities that could be subject to enforcement by Chinese authorities to include any activities overseas that endanger China's cybersecurity.

Penalty structure[15]

Instrument	Maximum penalty
PIPL (serious violations)	Up to CN¥50 million or 5% of global annual turnover
Amended CSL (serious consequences)	Up to CN¥2 million for the violating entity, and CN¥200,000 for the individuals directly responsible. If a breach has particularly serious consequences, up to CN¥10 million for the entity and CN¥1 million for the individuals responsible.
GenAI measures	Warnings, suspension of services, criminal referral

Board implications and actions

AI governance will increasingly be treated as a core dimension of cybersecurity and data compliance. The broadened extraterritorial reach heightens exposure for overseas entities whose activities intersect with China-based users or infrastructure. China is expected to maintain an agile approach to AI governance, seeking to balance technological innovation with data security, privacy protection and intellectual property rights. Directors should note that personal liability for senior management is codified in the PIPL, DSL and amended CSL.

[15]PwC. 10 ways China's new data rules will change your business. Accessed in April 2026.

A compliance map for the seven jurisdictions

Requirement	EU	US (Federal)	UK	Australia	India	Singapore	China
AI-specific law (binding)	✓ AI Act	⊗ Executive Orders and framework	◷ Expected H2 2026	⊗ Voluntary	⊗ Guidelines	⊗ Voluntary frameworks	✓ GenAI measures and amended CSL
Risk classification (mandatory)	✓	⊗	◷	⊗	⊗	⊗	⚠ Implicit
Board oversight expected	✓ Explicit	⚠ Implicit	⚠ Implicit	⚠ Implicit	⚠ Implicit (DPDPA)	✓ Monetary Authority of Singapore (MAS) for financial institutions	⚠ Implicit (PIPL/ CSL)
AI content labeling required	✓ (Aug 2026)	⊗	◷	⊗	⚠ Emerging	⊗	✓ Mandatory
Data protection law (relating to AI)	✓ General Data Protection Regulation (GDPR)	⚠ State-level	✓ UK GDPR	✓ Privacy Act	✓ DPDPA 2023	✓ PDPA 2012	✓ PIPL 2021
Maximum financial penalty	7% global turnover	Varies by state	Via sector laws	Via existing laws	₹250 crore (~$28M)	10% Singapore turnover	5% global turnover + CN¥10 million
Personal liability for directors	⚠ Via national law	⚠ Varies	⚠ Varies	⚠ Via existing law	⚠ Limited	✓ Criminal (PDPA)	✓ Fines and management bans
Extraterritorial reach	✓	⊗	◷ TBD	⊗	✓ DPDPA	⊗	✓ Broadened 2026
Agentic AI governance	⊗	⊗	⊗	⊗	⊗	✓ MGF	⊗

✓ = Existing/explicit ⊗ = Expected/under development ⚠ = Does not exist ◷ = Implicit (via other laws/regulations)

Governance frameworks and standards for boards

Boards do not need to build governance from scratch. Two internationally recognized frameworks provide a dual foundation:

1. ISO/IEC 42001:2023 — AI Management System (AIMS) standard

ISO/IEC 42001, published December 2023, is the first certifiable international standard for AI management systems. It specifies requirements using a Plan–Do–Check–Act methodology covering governance, risk management, transparency and ethical use, and contains 38 controls across 9 governance areas, applicable to all industries and entity sizes.

2. NIST AI Risk Management Framework (AI RMF) 1.0

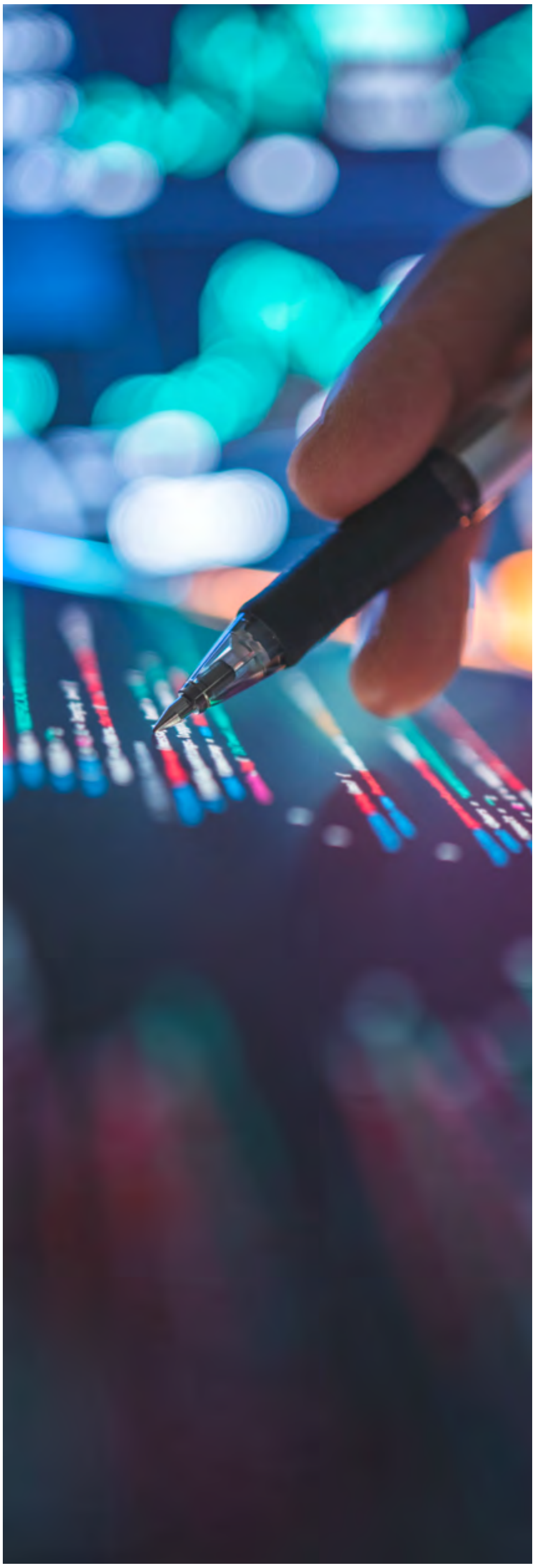
Published in January 2023, the voluntary framework comprises four iterative functions: Govern–Map–Measure–Manage. A Generative AI Profile (NIST AI 600-1) provides specific guidance. The framework is used internationally as a companion for EU AI Act compliance.

Complementary, not competing

ISO/IEC 42001 provides a certifiable, structured governance backbone. NIST AI RMF provides operational risk management functions. Together, they offer organizations a comprehensive governance architecture.

Board-level recommendation

Adopt ISO/IEC 42001 as the organizational governance backbone and integrate NIST AI RMF's risk functions for operational risk management and regulatory compliance mapping.



The board's AI governance action framework

Pillar 1: Establish a board-level AI oversight structure	Most boards still focus on education and risk awareness rather than embedding AI oversight into core operations. The National Association of Corporate Directors (NACD) concludes that boards are at an inflection point, transitioning from awareness to strategic, structured governance of AI within corporate decision-making. Deliverables: • Assign AI oversight to an existing committee (audit/risk) or establish a dedicated AI committee. • Mandate quarterly AI governance reporting to the board. • Require management to maintain a live inventory of AI systems for all jurisdictions.
Pillar 2: Build AI literacy at board level	Board members lacking AI literacy struggle to evaluate governance frameworks or identify red flags in vendor relationships. AI governance oversight does not require deep technical knowledge — it requires the same governance skills applied to financial risk, cybersecurity or regulatory compliance. Deliverables: • Commission annual board education sessions on AI developments. • Add AI governance expertise to director-selection criteria. • Engage external advisors for independent AI governance assessments.
Pillar 3: Codify AI governance	Deliverables: • Adopt a board-approved AI governance policy aligned to ISO/IEC 42001 and NIST AI RMF. • Establish clear accountability: Designate a Chief AI Officer or equivalent. • Document risk classifications for all deployed AI systems, mapped to jurisdictional requirements.
Pillar 4: Implement cross-jurisdictional regulatory compliance mapping	Boards operating in multiple jurisdictions face divergent and evolving requirements. The compliance map provides a snapshot of these. Organizations should develop dynamic compliance mapping that tracks: • EU AI Act phased implementation through 2027 • US state-level requirements by geography and sector • UK's anticipated legislation (H2 2026+) • India's DPDPA and sector-specific mandates (RBI, Securities and Exchange Board of India) • Singapore's evolving MAS guidelines for financial services • China's amended CSL and layered regulatory stack • Australia's Privacy Act automated decision-making reforms (December 2026)
Pillar 5: Monitor, measure and report	Despite widespread adoption of governance frameworks, maturity remains low. Recent research indicates that approximately 75% of organizations report having an AI governance process, but only 12% consider these processes to be mature, highlighting a significant gap between implementation and effectiveness.[16] Deliverables: • Define and mandate AI key performance indicators: return on investment (ROI) by business unit, compliance status and incident tracking. • Require an independent assessment of AI governance maturity annually. • Report AI governance metrics to the board alongside financial and cybersecurity reporting.

[16] Tushar Thakur. AI governance statistics 2026: Key risks, trends, and growth. TECHRT. 5 May 2026.

The cost of inaction

Risk category	Impact
Regulatory fines	EU AI Act: Up to €35 million or 7% of global turnover China PIPL: Up to 5% of global turnover India DPDPA: Up to ₹250 crore[17] Singapore PDPA: Up to 10% of Singapore turnover[18]
Market access	Noncompliant AI systems can be withdrawn from the EU market. China actively enforces content and labeling rules.
Director liability	China's PIPL, DSL and CSL impose personal fines and management bans on senior leaders. Singapore's PDPA includes criminal liability.
Competitive disadvantage	Organizations with structured AI governance frameworks significantly outperform peers on AI ROI.[19]
Shadow AI risk	Almost all AI-related breach victims have been shown to lack proper access controls. Unsanctioned AI tools proliferate outside formal governance channels.
Regulatory fragmentation	Organizations remain subject to an uneven mix of state requirements, federal enforcement through existing authorities and political uncertainty. Multijurisdictional exposure compounds compliance risk.

[17]DPDPA. DPDPA Penalties Explained: Rs 50 Crore to Rs 250 Crore Fines. 1 February 2026.

[18]Singapore Statutes Online. Personal Data Protection Act 2012.

[19]NTT DATA. 2026 Global AI Report: A Playbook for AI Leaders.

Strategic synthesis: Three models, one requirement

The seven jurisdictions represent fundamentally different approaches to AI governance:

	Prescriptive	Innovation-led	State-directed
Jurisdictions	EU	US, UK, Australia, India, Singapore	China
Philosophy	Regulate comprehensively by risk tier	Guide through principles, standards and sandboxes	Control the ecosystem through layered law
Board risk	Compliance deadlines with severe penalties	Regulatory fragmentation and rapid change	Multilaw overlap and personal liability
Trajectory	Majority enforcement from 2026	Moving toward binding standards	Deepening enforcement and extraterritorial reach

Every jurisdiction expects boards to:

- Know where AI is used in the organization
- Understand the risk classification of each AI system
- Demonstrate controls that are proportionate to the risk
- Ensure accountability at the senior leadership level

3 things to do in the next 90 days

2026 will mark a turning point, with boards and executive teams institutionalizing AI governance as a core competency.

The window for proactive action is narrowing.

We recommend every board take the following three actions within the next 90 days:

1. **Conduct an AI inventory and risk assessment**

   Map every AI system in use across all jurisdictions, classify these systems by risk tier and identify governance gaps against the compliance map.

2. **Adopt a formal AI governance framework**

   Align your framework to ISO/IEC 42001 and/or NIST AI RMF, with board-approved policy and clear accountability.

3. **Schedule board AI education**

   Ensure the full board achieves baseline AI literacy to ask the right oversight questions.

The question for directors is no longer whether AI governance matters but whether your board is ready.

DISCLAIMER: This paper is for informational and educational purposes only and does not constitute legal or regulatory advice. Organizations should consult qualified legal counsel for jurisdiction-specific compliance guidance. All data sourced from publicly available materials as of April 2026 with the support of AI.

Appendix A: Key regulatory instruments cited

Instrument	Jurisdiction	Year	Source
Regulation (EU) 2024/1689 — AI Act	EU	2024	eur-lex.europa.eu
EU Digital Omnibus Proposal	EU	Nov 2025	ec.europa.eu
GPAI Code of Practice	EU	Jul 2025	ec.europa.eu
EO 14179 — Removing Barriers to AI Leadership	USA (federal)	Jan 2025	whitehouse.gov
EO 14365 — National Policy Framework for AI	USA (federal)	Dec 2025	whitehouse.gov
National Policy Framework for AI	USA (federal)	Mar 2026	whitehouse.gov
California SB 53 (Frontier AI Transparency Act)	USA (state)	Effective Jan 2026	leginfo.legislature.ca.gov
Texas TRAIGA	USA (state)	Effective Jan 2026	capitol.texas.gov
Colorado AI Act (SB24-205)	USA (state)	Effective Jun 2026	leg.colorado.gov
AI Regulation White Paper	UK	Mar 2023	gov.uk
AI (Regulation) Bill [HL]	UK (proposed)	Reintroduced Mar 2025	parliament.uk
National AI Plan 2025	Australia	Dec 2025	industry.gov.au
AI6 Guidance for AI Adoption	Australia	Oct 2025	digital.gov.au
India AI Governance Guidelines	India	Nov 2025	meity.gov.in
DPDPA 2023	India	2023	meity.gov.in
RBI FREE-AI Committee Report	India (financial sector)	Aug 2025	rbi.org.in
MGF (second edition)	Singapore	2020; GenAI ed. 2024	pdpc.gov.sg

Appendix A: Key regulatory instruments cited (continued)

Instrument	Jurisdiction	Year	Source
MGF for Agentic AI	Singapore	Jan 2026	imda.gov.sg
National AI Strategy 2.0 (NAIS 2.0)	Singapore	Dec 2023	smartnation.gov.sg
AI Verify Testing Framework	Singapore	2022	aiverify.sg
Personal Data Protection Act 2012 (amended)	Singapore	2012; amended 2020	sso.agc.gov.sg
Cybersecurity Law (Amended)	China	2017; amended Oct 2025; effective 1 Jan 2026	npc.gov.cn
PIPL	China	2021	npc.gov.cn
DSL	China	2021	npc.gov.cn
Interim Measures for Generative AI Services	China	Jul 2023	cac.gov.cn
AI-Generated Content Labeling Measures	China	Mar 2025; effective Sep 2025	cac.gov.cn
ISO/IEC 42001:2023 — AI Management Systems	International	2023	iso.org
NIST AI Risk Management Framework 1.0	US/global	2023	nist.gov

NTT DATA