AI Governance in India: A Case Study

By: Ms. Astha Ojha

Capacity Building Division, NeGD

Introduction

The National e-Governance Division (NeGD), under the Ministry of Electronics & Information Technology (MeitY), continues to play a pivotal role in advancing the Digital India vision. Central to this effort is Capacity Building (CB), which equips government officials, technologists, and stakeholders with the knowledge and skills required to design, implement, and sustain innovative digital governance initiatives across the country.

This case study, "AI Governance in India", forms part of NeGD's ongoing commitment to document and disseminate best practices in emerging technologies, digital policy, and responsible innovation. Developed by internal experts at the Capacity Building Division, the study examines how India's legal frameworks, institutional mechanisms, and policy strategies are shaping a responsible and inclusive AI ecosystem. It provides a comprehensive exploration of the country's evolving approach to governing artificial intelligence—highlighting the balance between innovation, transparency, fairness, and accountability.

As AI technologies become deeply embedded in public service delivery, digital platforms, and citizen-facing applications, the imperative to ensure ethical, secure, and human-centric AI development grows stronger. This study evaluates both the opportunities and challenges posed by AI adoption, including issues of risk management, data governance, equity, explainability, and cross-sector implementation. Through this lens, it underscores the need for robust governance frameworks that can effectively address India's scale, diversity, and complex socio-economic landscape.

Our methodology integrates extensive research, analysis of legal and policy instruments, and insights from domain experts and stakeholders shaping India's AI governance discourse. This approach ensures that the study is grounded in practical experience, institutional realities, and current global benchmarks.

The objective of this repository is to serve as a valuable knowledge asset for policymakers, program managers, technologists, innovators, and implementers across government and industry. By enabling informed decision-making and fostering responsible AI deployment, it supports the broader Digital India initiative and contributes to the development of a transparent, accountable, and citizen-centric AI governance ecosystem.

Acknowledgment

The Capacity Building Division, NeGD, extends its sincere gratitude to Ms. Astha for developing this insightful and detailed case study titled AI Governance in India

The study's comprehensive examination of copyright enforcement, platform governance, and the interplay between Indian legal frameworks and global digital platforms has significantly enriched the understanding of content protection challenges in India's digital ecosystem.

We also acknowledge the valuable inputs and perspectives drawn from legal practitioners, digital content creators, and policy stakeholders, whose experiences and observations helped illuminate the real-world implications of automated copyright enforcement mechanisms, fair dealing under Indian law, and platform liability regimes. Their contributions were instrumental in contextualizing the practical impacts of technologies such as automated content identification systems and notice-and-takedown workflows on creators and users.

Furthermore, we extend our deepest appreciation to the internal experts at NeGD who meticulously reviewed this document. Their rigorous scrutiny ensured alignment with pedagogical standards, factual accuracy, and consistency with relevant statutory frameworks, including the Copyright Act, 1957, the Information Technology Act, 2000, and evolving global approaches to content moderation and digital governance. Their efforts have strengthened the document's enduring value as a resource for capacity building among policymakers, legal professionals, and digital governance stakeholders.

Disclaimer

This case study has been developed by the National e-Governance Division (NeGD) under its Capacity Building mandate for the purpose of knowledge sharing and academic reference. The information presented herein has been compiled from official government sources, project documents, and interviews with relevant stakeholders involved.

While every effort has been made to ensure the accuracy and reliability of the information, this document is intended for educational and illustrative purposes only. It should not be interpreted as an official policy statement or a guideline for implementation. The views and conclusions expressed are those of the author and contributors based on their analysis and do not necessarily reflect the official position of the Ministry of Electronics & Information Technology (MeitY) or the National e-Governance Division (NeGD).

The commercial use of this material is strictly prohibited. This case study is meant to be used as a learning tool for government officials, trainees, and individuals interested in e-Governance and public policy.

Any reproduction or use of this material must include proper attribution to 'National e-Governance Division (NeGD).' All intellectual property rights remain with NeGD unless otherwise specified.

AI Governance in India: A Case Study

Executive Summary

India's journey towards becoming a digital powerhouse began decades ago. It started with early steps like installing its first computer at the Indian Statistical Institute back in 1955, and continued with steady investments that helped build the strong, world-class digital infrastructure the country is known for today. For example, India's Aadhaar program is "the world's largest digital identity programme," with over 138 crore (1.38 billion) identities issued. These foundations have supported a large and growing AI ecosystem: India now ranks first globally in AI skill penetration (AI-skilled workforce) (Dr Nivash Jeevanandam, 2024) and is among the top economies in private AI investment. In this regard, India AI Governance Guidelines released by the Ministry of Electronics and Information technology (MeitY) in July 2025, provide a framework that balances AI innovation with accountability, and progress with safety (MeitY, 2025). It reflects a strategic and collaborative approach to governing AI, built around seven guiding principles, or "sutras": Trust, People First, Innovation over Restraint, Fairness and Equity, Accountability, Understandable by Design, and Safety, Resilience, and Sustainability. Together, these principles aim to ensure that AI is built in a way that stays human-focused, fair, and transparent across all sectors. But as AI grows rapidly, it also creates new governance challenges. India now needs to balance its democratic values and socio-economic priorities, such as supporting marginalized communities, protecting people's rights, and ensuring security, with the fast pace of technological progress.

This case study looks at how India's AI governance system is taking shape, including its current laws, national strategy documents, the new IndiaAI Mission, and global best practices. It also highlights the gaps that remain and offers recommendations to help strengthen oversight and accountability.

India's AI governance is structured around six pillars: Infrastructure (expanding data and compute access and leveraging Digital Public Infrastructure), Capacity Building (education, training, awareness), Policy & Regulation (balanced and agile frameworks with targeted law amendments), Risk Mitigation (India-specific risk assessment and voluntary compliance), Accountability (graded liability, transparency, enforcement), and Institutions (whole-of-government approach with bodies like AI Governance Group (AIGG), Technology Policy Expert Committee (TPEC), and AI Safety Institute (AISI)) (PIB, July 2024, n.d.).

Learning Objectives

This case study aims to help readers understand:

1. How India is currently governing artificial intelligence using existing legal, policy, and institutional frameworks;

2. Whether India's AI governance approach adequately balances innovation with accountability, transparency, and social equity;

3. What governance gaps remain in India's AI ecosystem as AI adoption scales across high-risk sectors, and;

4. What policy and institutional interventions could strengthen AI oversight without stifling innovation.

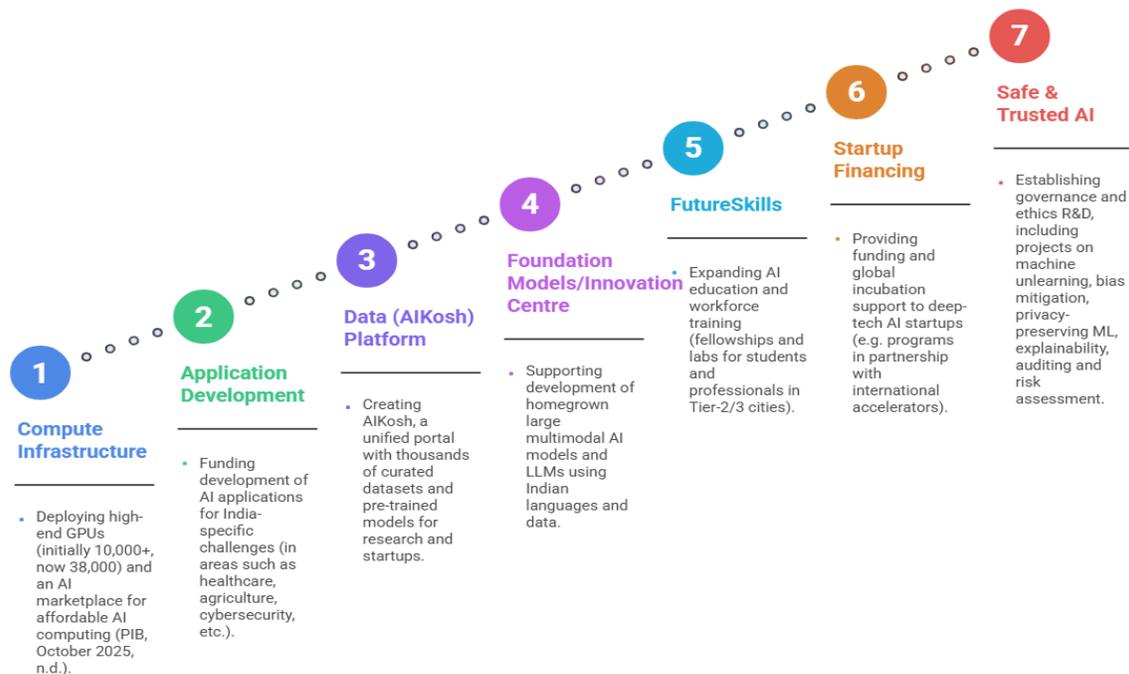## Legislative and Policy Foundations

Existing Legal Framework- India regulates AI only indirectly, using laws that are already in place. For example, the Information Technology Act of 2000 defines "computer resources" very broadly under Section 2(1)(k), as computer, computer system, computer network, data, computer database or software. This means AI systems end up falling under its cyberlaw provisions. In 2023 India enacted a dedicated data privacy law, the *Digital Personal Data Protection Act, 2023*, which governs processing of digital personal data. Other recent legal reforms (e.g. the *Bharatiya Nyaya Sanhita*, 2023, reforming the penal code) and longstanding laws (e.g. the Copyright Act, 1957) provide additional context, but do not address AI specifically. Thus, at present India relies on adapting existing laws and policies to AI use cases.

An upcoming amendment to the Information Technology Act may also introduce rules specifically for synthetic data. As AI models rely more and more on generated or anonymized datasets, the law needs to treat synthetic data as a regulated digital resource. Doing so would make it clearer who is responsible for creating, labeling, and using such data, helping to support innovation while also preventing misuse, such as deepfakes or data poisoning. This would cover non-personal, but AI-generated datasets that can still affect people's privacy and trust.

Strategic Policy Frameworks- In 2018, NITI Aayog released "*AI for All*," India's National Strategy for Artificial Intelligence, which highlighted inclusive growth and positioned the country as a key hub for AI solutions tailored to the needs of emerging economies. That strategy identified five priority sectors (healthcare, agriculture, education, smart cities/infrastructure, and smart mobility) and envisioned four foundational pillars (research & development, talent and reskilling, data and infrastructure, and ethics/regulation) to drive innovation (Niti Aayog, 2018). In early 2024 the Union Cabinet approved the **IndiaAI Mission**, allocating ₹10,371.92 crore over five years (PIB, March 2024, n.d.).

The IndiaAI Mission establishes a structured implementation plan with seven integrated pillars:

IndiaAI Mission Pillars

1 Compute Infrastructure
- Deploying high-end GPUs (initially 10,000+, now 38,000) and an AI marketplace for affordable AI computing (PIB, October 2025, n.d.).

2 Application Development
- Funding development of AI applications for India-specific challenges (in areas such as healthcare, agriculture, cybersecurity, etc.).

3 Data (AIKosh) Platform
- Creating AIKosh, a unified portal with thousands of curated datasets and pre-trained models for research and startups.

4 Foundation Models/Innovation Centre
- Supporting development of homegrown large multimodal AI models and LLMs using Indian languages and data.

5 FutureSkills
- Expanding AI education and workforce training (fellowships and labs for students and professionals in Tier-2/3 cities).

6 Startup Financing
- Providing funding and global incubation support to deep-tech AI startups (e.g. programs in partnership with international accelerators).

7 Safe & Trusted AI
- Establishing governance and ethics R&D, including projects on machine unlearning, bias mitigation, privacy-preserving ML, explainability, auditing and risk assessment.
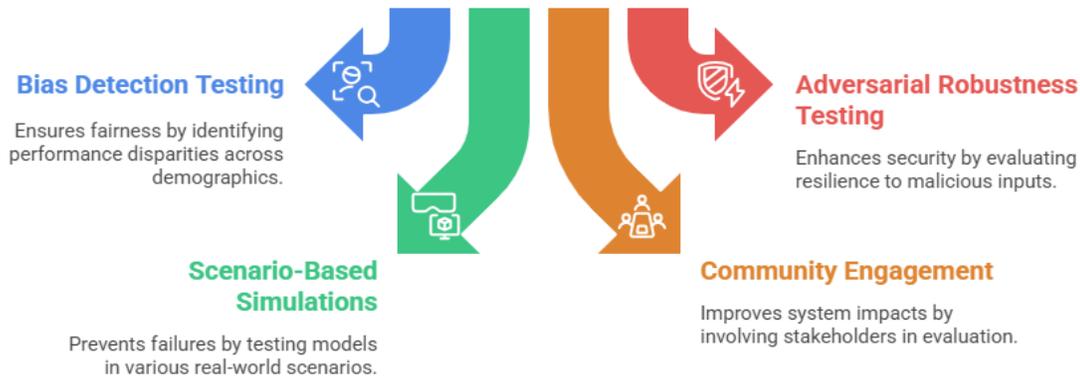
These national initiatives are complemented by other programs (e.g. Centres of Excellence for AI in key sectors, AI competency framework for government officials, and a planned AI Research College). Overall, India's strategy marries a focus on **"AI for inclusive growth"** with concrete investments in infrastructure, talent, data, and responsible development. (For example, the government emphasizes that AI is increasingly reaching citizens in rural and urban India – from improving access to medical care in remote areas to helping farmers make crop decisions.)

AI Testing and Accountability Mechanisms

A key recommendation is to embed *structured testing and evaluation* of AI systems as a formal part of governance. Global best practices now emphasize "red teaming", adversarial testing, to surface biases, errors, and unintended harms. UNESCO's recent **"Red Teaming AI for Social Good"** playbook (2025) presents AI red teaming as a practical methodology for systematically probing generative AI systems and exposing discriminatory or unsafe behaviors (Chowdhury et al., 2025). In line with this, India can adopt regular testing protocols such as:

Which AI testing protocol should be adopted?

Bias Detection Testing — Ensures fairness by identifying performance disparities across demographics.

Adversarial Robustness Testing — Enhances security by evaluating resilience to malicious inputs.

Scenario-Based Simulations — Prevents failures by testing models in various real-world scenarios.

Community Engagement — Improves system impacts by involving stakeholders in evaluation.

These practical testing approaches go beyond high-level principles, creating tangible assurance that AI products behave safely. They may be adopted in both Government and industry settings, with results feeding into a shared knowledge base (e.g. an AI incident database or public risk registry).

Core Governance Components

Accountability and Roles: India's governance framework needs clear assignment of responsibilities. AI developers and deploying agencies should be legally accountable for harms caused by their systems. For example, requirements could mandate developers to document system design (model cards) and track decisions made during deployment (audit trails). Data providers (especially of sensitive or personal data) and model producers (e.g. foundation model creators) must also be subject to standards of fairness, privacy, and transparency. Regulatory bodies at the national and state levels should be given authority to review AI systems. Multi-disciplinary oversight committees (involving experts from technology, law, social sciences and affected communities) can help mediate between innovation and public interest.

Standards and Evaluation: Formal technical standards (voluntary or mandatory) should be developed to specify benchmarks for safety, robustness, and transparency. Industry consortia and standards bodies (like the Bureau of Indian Standards) can draft codes of practice (e.g. for explainability, cybersecurity, data quality). Conformity assessment procedures – such as third-party audits or certifications – may be required for high-risk applications. Continuous monitoring is also essential: regulators could require post-deployment surveillance to detect drift and emergent risks over the AI system's lifecycle.

Coordination and Governance: India's federal structure and multi-ministerial bureaucracy present both opportunities and challenges. AI policy must be coordinated across central ministries (e.g. IT, Home Affairs, Health, Finance) as well as state governments. A possible mechanism is

an inter-ministerial AI coordination council (similar to existing ICT committees) chaired by a senior official (e.g. Cabinet Secretary) to align strategy and share best practices. Dedicated technical secretariats, staffed with trained AI experts, can support policymaking and review. Parliamentary or expert panels could provide democratic oversight of AI laws. Judicial training programs will also be needed to prepare courts for AI-related litigation (e.g. on liability or rights issues).

Trust is the Foundation: Trust must be embedded across the AI value chain, in technology, organizations, institutions, and users, for AI benefits to be realized at scale. AI systems should empower individuals and reflect their values with human oversight essential for accountability. It should prioritize responsible innovation over unnecessary caution; promote inclusive development and avoid discrimination against marginalized communities; assign responsibility clearly based on function and risk. AI systems should also provide explanations understandable to users and regulators and build safe, robust, and environmentally sustainable AI systems.

Transparency and Compliance: Increasing transparency across the AI value chain, developers, deployers, users, is essential for regulatory effectiveness. Voluntary compliance frameworks including regular audits, self-certifications, and public disclosure of risk mitigation efforts are recommended. Regulators should focus on preventing real harms through risk-based, flexible policy instruments, while supporting innovation and adopting techno-legal solutions.

Identified Gaps and Needs

Despite these efforts, several gaps remain:

Transparency Deficits: Many AI systems lack transparency. Indian users rarely receive model documentation or clear explanations of AI-driven decisions. This reduces accountability. For instance, without mandated "model cards" or clear documentation, regulators cannot easily audit system behavior. Explaining decisions (especially in domains like credit scoring or healthcare) is critical for trust but currently under-enforced.

Fragmented Policies: Existing policies are scattered across departments (cyberlaw under MeitY, healthcare data under Health Ministry, financial regulations under RBI, etc.). This can create overlap or loopholes. A coherent AI policy (possibly a national AI Act or omnibus regulation) could help unify these domains. Close coordination is needed to avoid conflicting rules.

Enforcement Capacity: Administrative agencies (both Central and State) generally lack technical AI expertise. There are few trained auditors or investigators for AI-specific harms (e.g. algorithmic bias or privacy breaches). Investment in regulatory capacity and digital infrastructure is needed to operationalize oversight plans.

Data and Equity Concerns: India's diversity (many languages, low-resource populations, rural users) means that AI risks can exacerbate existing inequities. For example, an AI health app might work well in English but fail for rural clinics without language support. Governance must explicitly

address equitable access and bias mitigation for India's varied contexts. Synthetic data, if properly governed, could help reduce data scarcity and bias by representing under-sampled populations. However, without legal guidance under the IT Act or related instruments, its misuse may amplify misinformation or privacy risks. Explicit governance for synthetic data generation and validation standards should thus form part of India's AI risk management strategy.

Risk Management and Accountability: AI systems pose risks including malicious use (deepfakes, model poisoning), bias and discrimination, transparency failures, systemic risks, loss of control, and threats to national security. The guidelines emphasize a need for a customized risk assessment framework reflecting India's socio-cultural context. There is a call for an AI incident reporting system to monitor and mitigate harms, and accountability mechanisms should involve clear legal enforcement and voluntary market-led approaches like transparency reports and grievance redressal.
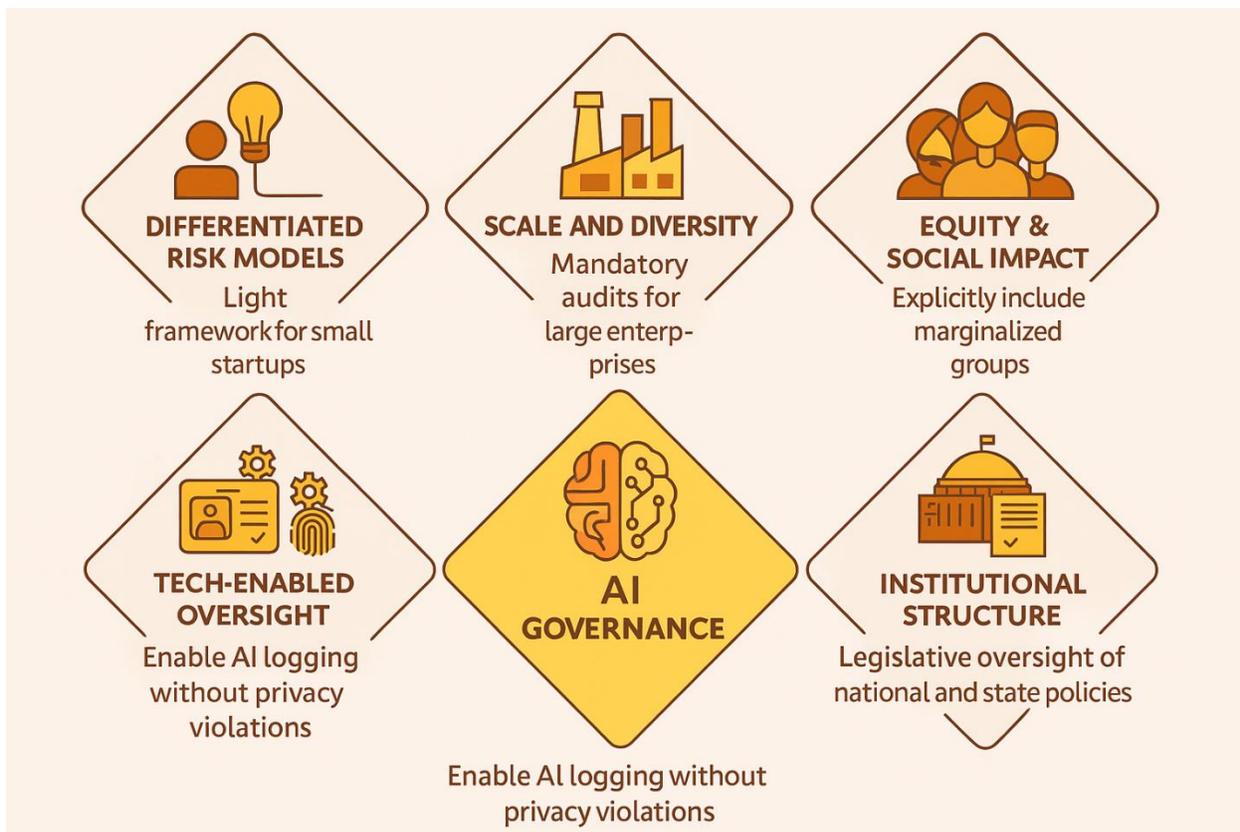
International Best Practices

India can draw lessons from leading AI governance models abroad:

European Union – Risk-Based Regulation: The EU's AI Act (Regulation 2024/1689) implements a *tiered risk approach*. AI systems are categorized into four levels – *unacceptable*, *high*, *limited*, and *minimal* risk, each with corresponding rules. Unacceptable-risk systems (e.g. social scoring, subliminal manipulation) are banned, while high-risk systems (e.g. critical infrastructure, certain biometric uses) face strict requirements (risk management, certification, human oversight). Lower-risk categories impose transparency obligations or no additional rules. Key features India could emulate include: a formal risk classification scheme; mandatory conformity assessments for high-risk AI; multi-level governance (EU central and member states); and post-market surveillance mechanisms to monitor deployed systems. This enables *proportionate regulation* targeting truly risky applications, rather than blanket bans (Austrian Regulatory Authority for Broadcasting and Telecommunications, n.d.).

Singapore – Practical Self-Regulation: Singapore's Model AI Governance Framework (first released 2019, updated 2020 (*PDPC | Singapore's Approach to AI Governance*, n.d.)) takes a largely voluntary, principles-based approach. The framework provides clear, **implementable guidance** on issues like transparency, explainability, and data governance. It is sector-agnostic and regularly updated. Singapore also developed *AI Verify*, a toolkit for companies to test AI systems against 11 common ethical principles. India can adapt this model by promoting *self-assessment tools* and best-practice guides for firms, focusing on broad accountability principles rather than heavy regulation. Voluntary frameworks can seed a culture of responsibility while standards mature.

Recommendations

Adaptations for India: In integrating these approaches, India's framework should account for local needs. For instance:

DIFFERENTIATED RISK MODELS
Light framework for small startups

SCALE AND DIVERSITY
Mandatory audits for large enterp-prises

EQUITY & SOCIAL IMPACT
Explicitly include marginalized groups

TECH-ENABLED OVERSIGHT
Enable AI logging without privacy violations

AI GOVERNANCE

INSTITUTIONAL STRUCTURE
Legislative oversight of national and state policies

Enable AI logging without privacy violations

(i) **Differentiated Risk Models:** Because India is both an AI developer (tech export hub) and a deployer (massive user base), risk assessments should consider an AI product's origin, use case, and developer capacity. Requirements for small startups might be lighter to avoid stifling innovation.

(ii) **Scale and Diversity:** Regulatory requirements (like mandatory audits) should scale with organization size and risk. Robust oversight might be mandatory for large enterprises, while smaller companies could follow simpler guidelines.

(iii) **Equity and Social Impact:** Risk frameworks must explicitly include social equity. Before approval, high-risk AI (in healthcare, policing, employment, etc.) should be evaluated for impacts on marginalized groups (e.g. by requiring social impact statements).

(iv) **Institutional Structure:** Create a federated governance structure: national AI policy coordinated by Central Government, with empowered roles for State Governments in implementation (e.g. local surveillance of state-level AI deployments). Ensure **parliamentary oversight** (through legislative committees or audits) for transparency. Provide specialized training and ethical review capabilities to courts to handle AI-related cases.

(v) **Tech-Enabled Oversight:** Use India's digital infrastructure (Aadhaar, UPI, DigiLocker, etc.) to aid governance. For example, AI deployments could be logged via the unified ID system, enabling traceability. Automated monitoring tools (using AI to audit AI) can flag anomalies. At the same time, privacy-preserving techniques (like differential privacy) should be applied so that oversight does not compromise individual data rights.

Sectoral Priorities

Governance must also address sector-specific concerns:

(i)   **Healthcare:** AI in healthcare holds promise for diagnostics and telemedicine but poses risks to patient safety and privacy. Key governance priorities include rigorous *clinical validation* of AI tools (pre- and post-deployment), fairness testing across gender, caste, and socio-economic groups, and strict data protection for health records. There should be clear accountability rules when AI aids medical decisions (e.g. guidelines on physician override). Additionally, policies must ensure AI-driven healthcare does not deepen inequities (for example, by bias toward urban populations). Red teaming in healthcare AI should test for worst-case scenarios (misdiagnosis risks, privacy leaks) across diverse patient data.

(ii)   **Financial Services:** In finance, AI is used for credit scoring, insurance, trading and more. Governance must enforce *algorithmic fairness* to prevent discrimination in lending or insurance. Regulators should monitor systemic risks from AI-driven market strategies (e.g. automated trading feedback loops). Consumer protection rules must mandate explainability for AI-based decisions (why was a loan denied?), and robust security to protect sensitive financial data. Red teaming can help identify adversarial exploitations (e.g. gaming credit models) and ensure compliance with fairness mandates.

(iii)   **Agriculture:** AI tools (like crop-prediction models or autonomous equipment) target India's vast rural sector. Governance here must balance innovation with farmer protection. Key issues include: *data privacy* (farmers' land/yield data is sensitive), *access and affordability* of AI tech for smallholders, and *respect for traditional knowledge*. Environmental impacts of AI (e.g. automated pesticide use) should be monitored. Evaluations should test AI solutions under low-connectivity conditions and local languages. Impact assessments can ensure that AI adoption in agriculture truly improves livelihoods without unintended harms (e.g. reducing crop diversity).

Conclusion

India's AI governance model is gradually taking shape, combining what already works with new ideas and institutions. Early efforts, like the IndiaAI Mission, specialized centers of excellence, and a range of policy initiatives, have created a solid starting point for building AI responsibly. But keeping this momentum will require steady political support, stronger regulatory know-how, and meaningful involvement from everyone who has a stake in the future of AI: businesses, researchers, civil society groups, and everyday citizens.

As technology evolves, India's approach will need to evolve with it. Rules and standards can't remain static, they'll have to be updated as new tools emerge and society's expectations change.

At the same time, India stands to gain by staying active in global AI conversations, sharing its experiences, learning from others, and helping shape international norms, all while preserving the flexibility to craft policies that reflect its own realities.

In the end, with thoughtful oversight, collaboration across fields, and policies grounded in evidence, India can use AI's potential to drive inclusive and meaningful growth. By tying its "AI for All" vision to strong governance and democratic values, India hopes to show that technological innovation can advance while still protecting people's rights and promoting fairness for all.

References

Austrian Regulatory Authority for Broadcasting and Telecommunications. (n.d.). *Risk leveles of AI systems | AI Service Desk*. RTR. Retrieved November 10, 2025, from https://www.rtr.at/rtr/service/ki-servicestelle/ai-act/risikostufen_ki-systeme.en.html

Chowdhury, R., Skeadas, T., Lakshmi, D., & Amos, S. (2025). *Red teaming artifical intelligence for social good: The playbook* (D. Cliche & S. Andrews, Eds.). United Nations Educational, Scientific, and Cultural Organization.

Dr Nivash Jeevanandam. (2024, December). *India leads global AI talent and skill penetration*. IndiaAI. https://indiaai.gov.in/article/india-leads-global-ai-talent-and-skill-penetration

MeitY. (2025, July). *India AI-Governance Guidelines*. https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc2025115685601.pdf

Niti Aayog. (2018). *National Strategy for Artificial Intelligence*.

PDPC | Singapore's Approach to AI Governance. (n.d.). Retrieved November 10, 2025, from https://www.pdpc.gov.sg/help-and-resources/2020/01/model-ai-governance-framework

PIB, July 2024. (n.d.). *Government of India taking measures to enhance the reach of Indian Digital Public Infrastructure*. Retrieved November 10, 2025, from https://www.pib.gov.in/www.pib.gov.in/Pressreleaseshare.aspx?PRID=2037598

PIB, March 2024. (n.d.). *Cabinet Approves Ambitious IndiaAI Mission to Strengthen the AI Innovation Ecosystem*. Retrieved November 10, 2025, from https://www.pib.gov.in/www.pib.gov.in/Pressreleaseshare.aspx?PRID=2012355

PIB, October 2025. (n.d.). *Transforming India with AI*. Retrieved November 10, 2025, from https://www.pib.gov.in/www.pib.gov.in/Pressreleaseshare.aspx?PRID=2178092