Navigating the AI Revolution: Why India Needs Strong AI Governance

Daniela Combe,
Vice President, Emerging Tech Advocacy, IBM

Sandip Patel
Regional General Manager, IBM India and South Asia

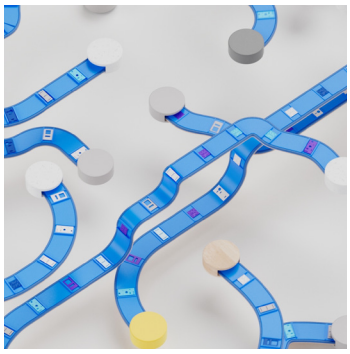
IBM has long championed India's AI growth, recognizing the nation's unique blend of technological prowess, dynamic talent, and strategic innovation initiatives. In its policy outlook, IBM highlights India's potential to lead the global artificial intelligence (AI) revolution, supported by a thriving information technology ecosystem and ambitious government programs like the National AI Strategy[1].

IBM's belief in India's AI journey is further reinforced by its commitment to building a trusted and open innovation ecosystem, where collaboration across sectors fosters inclusivity and democratizes access to transformative AI technologies. We believe open innovation and AI models that are open are essential for advancing scientific discovery and ensuring that the benefits of AI are accessible to as many people as possible. Such an approach promises to democratize access to transformative technologies for the 1.3 billion people in India. Generative AI, particularly foundation models, which require extensive compute and data resources, make it susceptible to centralization, threatening the equitable distribution of its benefits[2].

India stands on the brink of a significant AI-driven transformation, and with the implementation of well thought out regulations, it has the potential to spearhead the rapid growth currently unfolding in the sector. According to a recent IDC study, AI spending in India is projected to reach $6 billion by 2027[3], growing at a compound annual growth rate of over 33% from 2022 to 2027. This growth is fueled by India's vibrant startup ecosystem, which has seen the rise of over 150 generative AI startups, such as Krutrim AI and Sarvam AI[4], with substantial funding support. And the Indian government's initiatives, such as the National AI Strategy and the INDIAai Mission, further underline the country's commitment to fostering AI innovation, with over $1.25 billion allocated to support indigenous AI solutions.

Generative AI, in particular, holds immense promise for India's economy across multiple sectors, from agriculture and healthcare to finance and education. With a rapidly expanding AI ecosystem, supported by global partnerships and substantial investments, India is well-positioned to see the benefits of this innovative technology. In order to enable broad adoption of AI and thereby harness the full potential of AI, India must adhere to strong AI governance practices which protect society and sensitive data without hindering future innovations.

AI as a force multiplier for the government



In a recent roundtable conversation[5] convened by The Partnership for Public Service, in collaboration with the IBM Center for the Business of Government, leaders in government service delivery discussed the transformative potential of AI in government. AI was widely recognized as a powerful force multiplier, capable of enabling federal programs to deliver benefits more efficiently and accurately. Its potential for automating repetitive tasks and generating code could revolutionize how government builds and maintains IT infrastructure. AI offers the possibility to free civil servants from routine processes, allowing them to focus on more creative and impactful interactions with citizens.

However, the leaders acknowledged that AI's power can magnify adverse outcomes, such as systemic bias and performance issues, if not implemented responsibly. This highlights the urgent need to address fairness, security, and transparency through governance frameworks.

Importance of AI governance frameworks

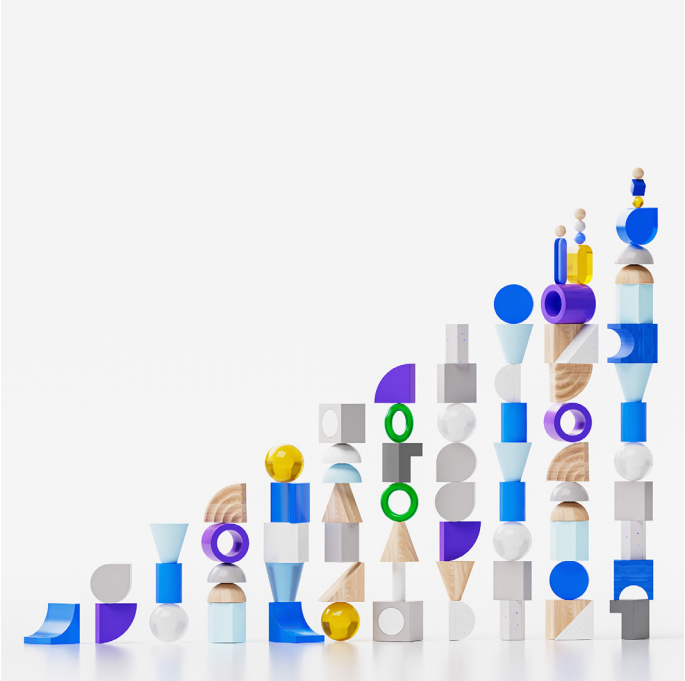
As governments across the globe continue to develop and implement AI regulations, they should concurrently prioritize the creation of an AI governance framework to guide responsible AI development and deployment. This framework should also provide immediate guidance on ethical AI use, transparency, and accountability, ensuring that innovation progresses safely while formal regulations are being finalized.

AI governance refers to the guardrails that ensure AI tools and systems are safe and ethical. It establishes the frameworks, rules and standards that direct AI research, development and application to ensure safety, fairness and respect for human rights. AI governance encompasses oversight mechanisms that address risks like bias, privacy infringement, and misuse while fostering innovation and trust. A human-centric approach for AI requires the involvement of a wide range of stakeholders, including AI developers, users, policymakers, and ethicists, ensuring that AI-related systems are developed and used to align with society's values.

AI governance is essentially the set of processes, policies, and tools that bring together diverse stakeholders across data science, engineering, compliance, legal, and business teams to ensure that AI systems are built, deployed, used, and managed to maximize benefits and prevent harm. Since AI is a product of highly engineered code and machine learning created by people, it is susceptible to human biases and errors. Governance provides a structured approach to manage AI solutions and mitigate risk through monitoring and evaluation that allows for adjustment to prevent flawed or harmful decisions.

Moreover, AI governance is not just about ensuring one-time compliance; it's also about sustaining ethical standards. AI models can drift, leading to changes in output quality and reliability. In addition, business solutions leveraging or integrating AI models can drift from their intended metrics and purposes. Current trends in governance are moving beyond mere legal compliance towards ensuring AI's social responsibility, thereby safeguarding against financial, legal and reputational damage while promoting the responsible growth of technology.

Pillars of AI governance



AI governance is essential for managing rapid advancements in AI technology, particularly with the emergence of generative AI. Generative AI, which includes technologies capable of creating new content and solutions, such as text, images and code, has vast potential across many use cases. From enhancing creative processes in design and media to automating tasks in software development, generative AI is transforming how industries operate. However, with its broad applicability comes the need for robust AI governance.

The key pillars of responsible AI governance are essential for organizations to safeguard themselves and their customers. The following pillars can guide organizations in the ethical development and application of AI technologies:

- **Explainability:** AI systems should be transparent about the factors contributing to their algorithmic recommendations, tailored to the needs of diverse stakeholders with varying objectives. When an AI system impacts individuals significantly, it must be capable of explaining and contextualizing its conclusions. This involves making the system's functionality comprehensible even to non-experts, with documentation provided in an accessible format that includes confidence measures, error analyses, and procedural details. Trustworthy AI systems must not compromise transparency for user experience, as opaque AI erodes trust.

- **Fairness:** AI has the potential to help humans make fairer decisions by addressing biases and enhancing inclusivity. Fairness in AI means treating people equitably, free from biases that may arise from flawed algorithm design or biased data. Bias can stem from various sources, such as cultural or technical limitations, and can be exacerbated when AI is applied in contexts not anticipated during its development. Ensuring inclusivity involves fostering diverse development teams and considering different perspectives.

- **Robustness:** Robust AI systems are designed to withstand adversarial attacks and handle unexpected conditions without unintended harm. This includes protecting against vulnerabilities like data poisoning, where attackers manipulate training data to compromise system security. As AI systems are increasingly employed in critical decision-making roles, ensuring their security and robustness is paramount. Robust AI maintains reliability under various stressors, contributing to the overall trustworthiness of AI outcomes.

- **Transparency:** Transparency is crucial for fostering trust in AI systems. It involves providing clear insights into how the AI functions, its strengths, limitations, and the data it uses. Transparent AI systems disclose the nature of data collection, usage, storage, and accessibility, ensuring that users understand the purpose and mechanics of the AI they interact with.

- **Privacy:** AI systems must prioritize consumer privacy and data rights, offering clear data usage and protection assurances. Respecting privacy involves fully disclosing what data is collected, how it is used, and who can access it. AI operators should collect only the minimum necessary data, use it explicitly for stated purposes, and prevent misuse. Privacy settings should be transparent and accessible, enabling users to control how their data is managed. Effective data protection relies on privacy-focused design practices, including encryption and stringent access controls.

How Singapore is advancing AI governance

For example, Singapore's AI Verify Foundation successfully shows how collaboration between industry and government can create a robust AI governance framework. Launched by Singapore's Infocomm Media Development Authority, the AI Verify Foundation brings together companies, researchers, and policymakers to develop open source tools and frameworks that help organizations verify their AI systems' ethical and responsible implementation. With the idea of fostering an inclusive, global, open-source community, the initiative facilitates the development of AI governance testing frameworks that align with internationally recognized principles. This collaborative approach helps addresses both immediate and long-term AI governance challenges by combining the strengths of the public and private sectors.

The AI Verify initiative demonstrates that effective AI governance requires a concerted effort from multiple stakeholders across sectors and geographies. Through initiatives like AI Verify, industry leaders, policymakers, and researchers can work together to develop practical guidelines and testing standards that ensure the safe deployment of AI while fostering innovation. Singapore's initiative is a model for how the Indian government and the industry can jointly develop the necessary tools to create an AI-ready future.

IBM Products for AI Governance

IBM offers a comprehensive range of AI governance products[6], with watsonx.governance being a flagship solution designed to manage AI across various industries. This platform provides customizable tools to help organizations address critical concerns like risk management, data security, and ethical AI deployment across the AI lifecycle and facilitate regulatory compliance. Through integration with other platforms watsonx. governance enables businesses to streamline workflows, automate compliance checks, and ensure continuous monitoring of AI solutions, which is particularly valuable in high-stakes sectors like finance and healthcare. Its effectiveness lies in its ability to provide an end-to-end solution for AI lifecycle management, from development to deployment, ensuring that AI systems are transparent, accountable, and aligned with organizational goal. By offering automated workflows, audit trails, and risk assessment protocols, watsonx.governance allows companies to maintain control over their AI solutions while minimizing risks associated with model drift and biases.

[1]https://www.ibm.com/policy/wp-content/uploads/2024/02/FINALPolicy_AIinIndia-3.pdf
[2]https://www.idc.com/getdoc.jsp?containerId=prAP52380424
[3]https://analyticsindiamag.com/ai-highlights/gen-ai-startup-landscape-in-india-2024/
[4]https://indiaai.gov.in/article/global-indiaai-summit-2024-concludes-paving-way-for-india-s-leadership-in-ai-innovation
[5]https://www.businessofgovernment.org/blog/perspectives-ethical-use-artificial-intelligence-government
[6]https://www.ibm.com/downloads/cas/KXVRM5Q