IndiaAI – a MeitY initiative

इलेक्ट्रॉनिकी एवं
सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF
ELECTRONICS AND
INFORMATION TECHNOLOGY
सत्यमेव जयते

WORLD ECONOMIC FORUM

In collaboration with the Office of the Principal Scientific Adviser to the Government of India and BCG X

Shaping the AI Sandbox Ecosystem for the Intelligent Age

WHITE PAPER

AUGUST 2025

Images: Midjourney, Getty Images

Contents

Foreword 3

Executive summary 4

Introduction 5

1 Sandboxes in the Intelligent Age – what and why 6

1.1 Context and methodology 9

2 Enablers of AI innovation in India 10

3 Creating enablers through AI sandboxes 12

4 The framework for the AI sandbox ecosystem 14

4.1 Vision of the AI sandbox 14

4.2 Strategic framework: Guiding principles and structure 15

4.3 Operational framework: Translating strategy into action 17

5 A call to action 21

Conclusion 23

Appendix 24

Contributors 26

Endnotes 29

Foreword

S. Krishnan
Secretary, Ministry of Electronics and Information Technology (MeitY), Government of India

Ajay Sood
Principal Scientific Adviser to the Government of India

Jeremy Jurgens
Managing Director, Centre for Frontier Technologies and Innovation, World Economic Forum

Nipun Kalra
Managing Director, Senior Partner and India Head, BCG X

Artificial intelligence is advancing at a remarkable pace, shaped by breakthroughs in open-source generative AI models, autonomous systems and intelligent agents. These shifts are redefining the boundaries of technology and altering how societies, economies and institutions function. As AI capabilities continue to evolve, the question for countries is not whether to embrace them, but how to do so responsibly, swiftly and at scale.

For India, this moment presents a significant opportunity. With a unique combination of world-class digital public infrastructure (DPI), a vibrant start-up ecosystem, a rich base of technical talent and demographic scale, India is poised to lead globally in building AI solutions that are not only globally competitive but also socially impactful. Yet this promise can be realized only if we address the systemic challenges that hinder AI innovation.

The need of the hour is to build secure and controlled environments that enable agile experimentation while maintaining trust, safety and public interest. AI sandboxes provide such a pathway – allowing innovators to test and validate solutions in real-world settings with access to critical data, compute and regulatory guidance.

This white paper, *Shaping the AI Sandbox Ecosystem for the Intelligent Age*, provides a practical roadmap to design and establish AI sandboxes in ways that reflect India's unique needs and sectoral priorities, while ensuring that all the necessary safeguards are in place. Drawing on global benchmarking and deep stakeholder engagement, it lays the foundation for an AI ecosystem that accelerates innovation, strengthens public trust and supports India's journey towards socioeconomic prosperity.

Executive summary

This paper presents a national framework to enable responsible, inclusive and scalable AI innovation through controlled development and testing environments.

Artificial intelligence (AI) is rapidly transforming economies and societies, with advances in generative models, intelligent agents and autonomous systems opening new frontiers for growth. This rapid evolution presents countries with a dual imperative: to accelerate innovation while ensuring it remains responsible, inclusive and aligned with the public interest.

India is uniquely positioned to lead this transformation. With strong digital public infrastructure (DPI), a vibrant start-up ecosystem and a large, multilingual population, the country offers an ideal testbed for building and scaling AI solutions that address both domestic priorities and global challenges. However, India continues to face a few structural challenges – including limited access to localized datasets and compute infrastructure, a lack of standard validation frameworks and constrained support for early-stage start-ups.

AI sandboxes offer a timely solution to address the most critical of these challenges. They provide secure, controlled environments where innovators can test, validate and refine AI solutions using real-world data, infrastructure and regulatory guidance. Globally, such sandboxes have been deployed in regulatory, innovation-focused and hybrid formats across sectors such as healthcare, finance and education.

This white paper presents a comprehensive framework for catalysing the establishment of AI sandboxes. The framework has been developed through consultations with more than 20 experts, a multistakeholder workshop with over a dozen AI-first start-ups and global benchmarking of best practices. It comprises two key components:

1. A **strategic framework** that outlines five core layers of the AI sandbox ecosystem – infrastructure, data, models, innovation and governance – each embedding enablers for the creation of AI solutions and guardrails for responsible deployment.
2. An **operational framework** that defines four key phases for implementation:

– Defining the objectives and scope aligned with national and sectoral priorities

– Establishing multistakeholder governance and access protocols

– Designing and developing sandbox components, including datasets, compute infrastructure, models and validation tools

– Establishing the AI sandbox, tracking outcomes and scaling through structured adoption and commercialization pathways

The framework directly addresses five systemic challenges in India's AI ecosystem: (1) data accessibility and governance; (2) access to compute infrastructure; (3) model affordability and contextual representation, regulatory uncertainty and lack of awareness around validation mechanisms; (4) limited avenues for market access; and (5) limited ecosystem enablement. It positions sandboxes not merely as pilot environments but also as long-term national platforms that propel responsible AI innovation and deployment.

The paper concludes with a call to action for key stakeholders. The government can play a catalytic role by funding pilots and enabling national coordination. Industry has an essential role in contributing infrastructure, expertise and mentorship. Academia is critical for driving validation efforts and leading capacity-building initiatives. Start-ups are central to the sandbox's success through active participation, continuous feedback and co-development of scalable, real-world solutions. Regulators provide crucial oversight and guidance to shape safe and responsible experimentation environments.

Together, these efforts can help establish AI sandboxes as a cornerstone of India's AI strategy – positioning the country as a global leader in inclusive, scalable and trusted AI development.

Introduction

Balancing rapid innovation with social responsibility is imperative for nations in the Intelligent Age.

Artificial intelligence has the potential to significantly drive economic growth, offering substantial early-mover advantages to countries that proactively adopt a strategic approach to accelerating AI innovation.[1] The current early phase of AI development is characterized by rapid advances and widespread discussion, making it challenging to distinguish between hype and actual progress. Nonetheless, with its capacity to emulate human-like thinking and behaviour, there is little doubt that AI represents a transformative force.

For countries such as India, this presents a powerful opportunity to drive inclusive growth, enhance productivity and strengthen digital leadership. However, these gains come with significant risks – including algorithmic bias, privacy violations, safety concerns, regulatory uncertainty and most importantly the "unknown-unknown" risks. Balancing innovation with responsibility is now a global imperative. Nations must strike a careful balance – ensuring responsible design, development and adoption while rapidly building the infrastructure and institutional capacity required to promote AI innovation at scale.

While India is well positioned with its thriving start-up ecosystem, digital public infrastructure (DPI) and deep talent pool, systemic challenges – such as limited access to computing infrastructure (compute) and high-quality data, lack of awareness around regulations and a nascent innovation ecosystem – continue to hinder scalable AI innovation. At the same time, the fast-changing nature of AI demands agile experimentation mechanisms to evaluate new technologies and translate them into real-world value.

In response to this dual imperative, the **AI for India 2030** initiative was launched by the World Economic Forum's Centre for the Fourth Industrial Revolution India (C4IR India) in collaboration with the Ministry of Electronics and Information Technology (MeitY), the Office of the Principal Scientific Adviser (PSA) to the Government of India and the National Association of Software and Service Companies (Nasscom). The initiative brings together leaders in government, industry, start-ups and academia through a high-level advisory council of more than 20 experts to co-design approaches that enable responsible and inclusive AI adoption.

The advisory council's early deliberations highlighted the need for two foundational interventions to unlock AI's value in India:

- **AI playbooks:**[2] Actionable frameworks to guide sectoral AI adoption in priority sectors (such as in agriculture, healthcare and micro-, small and medium enterprises [MSMEs]), including use cases, readiness assessments and policy recommendations

- **AI sandboxes:** Frameworks for establishing safe and structured environments in which start-ups and innovators can test, validate and refine AI solutions using real-world data, compute infrastructure and regulatory guidance

Of these, the **AI sandbox workstream** was specifically envisioned to address the key challenges at the ecosystem level through agile, secure and collaborative testing mechanisms. As frontier technologies such as agentic AI,[3] physical intelligence, artificial superintelligence (ASI)[4] and autonomous systems continue to evolve, the need for trusted testbeds that support responsible innovation and real-world validation has only become more urgent.

> **India's demographic dividend is not just about people – it's about use cases. The next billion Indians don't want a chatbot – they want a doer. We should measure AI success not by model size, but by task completion at population scale. That's where sandboxes – if designed right – can be India's 'launchpads' for AI agents that serve Bharat.**
>
> AI for India 2030 member

1 Sandboxes in the Intelligent Age – what and why

AI sandboxes reduce risks, accelerate experimentation and bridge the gap between research and real-world deployment.

An AI sandbox is a controlled environment that allows innovators to safely develop, test and refine AI models and applications. The European Union AI Act 2024[5] defines an AI regulatory sandbox in the following terms: "'AI regulatory sandbox' means a controlled framework set up by a competent authority which offers providers or prospective providers of AI systems the possibility to develop, train, validate and test, where appropriate in real-world conditions, an innovative AI system, pursuant to a sandbox plan for a limited time under regulatory supervision."

The EU AI Act accords legal status to **AI regulatory sandboxes** and defines their objectives as well as some of the operational details. It is useful to recount here the provisions of the EU AI Act relating to sandboxes.

The following objectives for AI sandboxes set by the Act are universal, and highlight how innovation and regulatory development should be considered side by side.

a. Improving legal certainty to achieve **regulatory compliance with this regulation or, where relevant, other applicable Union and national law**

b. Supporting the sharing of **best practices** through cooperation with the authorities involved in the AI regulatory sandbox

c. Fostering **innovation** and **competitiveness** and facilitating the development of an AI ecosystem

d. Contributing to evidence-based **regulatory learning**

e. Facilitating and accelerating access to the Union market for AI systems, in particular when provided by **SMEs, including start-ups**

These objectives seek to promote innovation and progress from within the regulatory guardrails.

The other key features of the EU AI Act 2024 relevant to this study are outlined below. In this section, AI regulatory sandboxes are referred to as AIRS for brevity:

a. **How many AIRS?** It is appropriate to establish an AIRS at the national level and additional AIRS at the subnational level in AI-producing countries. The Federal Government may establish an exclusive AIRS for validating AI solutions designed for the public sector.

b. **Exit report:** The competent authority of the AIRS shall issue an "exit report" to the developer or start-up whose solution has passed all the test criteria established by the AIRS. This exit report, serving as a form of validation certificate, can be used as a credential to support product marketing and outreach.

c. **Equitable access to AIRS services:** Clear and transparent eligibility criteria shall be prescribed for developers and start-ups to enter the AIRS. The time limit for remaining in the AIRS may be determined based on the complexity of the problem being addressed and the current stage of the solution design.

d. **Free service:** The services of AIRS shall be provided **free**, except for the cost of specialized materials required for testing a specific use case.

e. **Facilities at AIRS:** AIRS shall have the infrastructure, tools and **capabilities** for testing, benchmarking, assessing and explaining the dimensions of AI systems – accuracy, robustness, trustworthiness and cybersecurity – besides measures to investigate risks.

f. **Personal data processing:** Personal data collected by an agency for some purposes may be used for AI systems in AIRS, subject to certain conditions, which stipulate that public interest should be served by the proposed AI system; for instance, relating to public safety, public health, healthcare, transportation, critical information infrastructure, networks, climate action, energy sustainability and, especially, the **efficiency and quality of public administration and public services**.

g. **Monitoring systems** shall be put in place.

h. Personal data must be processed in **confidential computing rooms**.

Most of the operational provisions of the Act are useful to countries seeking to establish an AI sandbox ecosystem.

Depending on their core objective, sandboxes worldwide can typically be classified into three categories:[6]

1 **Regulatory sandboxes**

Provide a supervised space to pilot AI solutions under the guidance of regulators, enabling the early identification of risks and compliance pathways before full-scale deployment.

Particularly useful in sectors such as finance and healthcare, where safety and compliance are critical.

2 **Innovation (or operational) sandboxes**

Offer shared access to data, compute capacity and other resources, enabling rapid prototyping and collaborative development of AI applications.

Especially relevant in sectors such as agriculture, education, logistics and MSMEs, where rapid experimentation can unlock scalable solutions.

3 **Hybrid sandboxes**

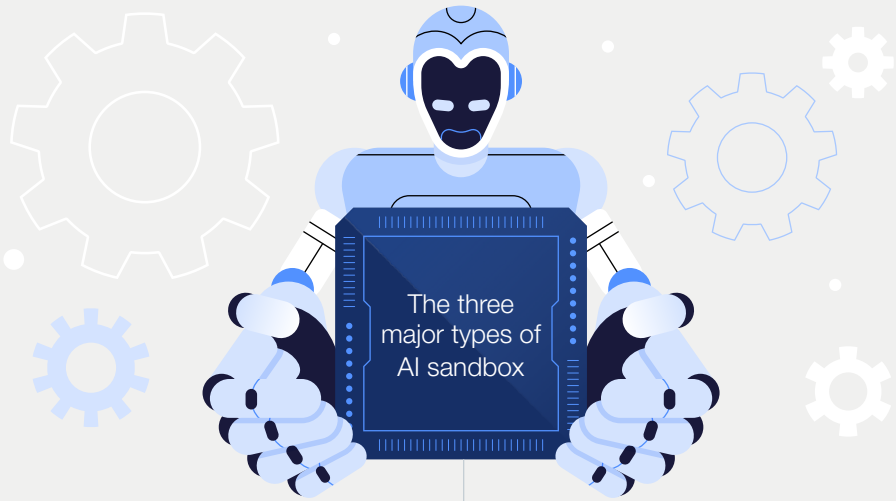
Combine the benefits of innovation and regulatory models – promoting experimentation while ensuring alignment with ethical, safety and policy frameworks.

Well suited to integrated domains such as digital health, fintech and smart governance, where both agility and oversight are necessary.

Globally, countries such as Norway,[7] Malaysia,[8] Brazil,[9] Singapore,[10] the United Kingdom[11] and Spain[12] are already adopting sandbox models to advance innovation and safeguard the public interest.

AI sandboxes have the potential to act as critical enablers for accelerating India's AI innovation while embedding trust, safety and inclusiveness into the ecosystem. This paper examines their relevance in the Indian context and proposes a framework to guide the establishment and operationalization of AI sandboxes.

FIGURE 1 | **The three major types of AI sandbox**



1 Regulatory sandbox	2 Innovation sandbox	3 Hybrid sandbox
Example Norway Regulatory Privacy Sandbox	**Example** Qatar MCIT AI Sandbox	**Example** Malaysia National Technology and Innovation Sandbox
Purpose Promote the development and implementation of ethical and responsible AI from a privacy perspective	**Purpose** Provide a flexible environment for developers, innovators and businesses to experiment with and develop AI-driven solutions	**Purpose** Accelerate companies to launch advanced technology applications while providing regulatory relaxation during development
Primary stakeholders Data Protection Authority, regulatory authorities, external experts	**Primary stakeholders** Developers, businesses, researchers, AI solution architects and data experts (mentors)	**Primary stakeholders** Developers, regulators, industry, tech experts, investors, facility providers, market access partners
Core components Regulatory assessment, mentorship	**Core components** Low-code/no-code IDE, P2P collaboration, expert mentorship	**Core components** Testbed, market access, funding, capacity-building, regulatory support, mentorship

Source: World Economic Forum analysis

1.1 Context and methodology

To create a practical and actionable framework for establishing AI sandboxes in India, the World Economic Forum, under the guidance of the AI for India 2030 Advisory Council, constituted a multistakeholder Expert Group for the AI sandbox workstream (see Contributors for the composition of the Advisory Council and Expert Group). The Expert Group brought together key perspectives from across the AI ecosystem – government officials, industry leaders, start-up founders, researchers and global experts. This methodology helped surface insights grounded in the Indian context while drawing from global experiences to shape a forward-looking AI sandbox framework.

Following the Expert Group's recommendation, the team undertook the following three activities:

- **A multistakeholder workshop held on 25 February 2025** in Bengaluru comprising leading AI-first start-ups (see Contributors for the list of start-ups) in sectors such as healthcare, agriculture, education and logistics, along with officials from the government of Karnataka, aimed at identifying on-the-ground barriers to innovation.
- **Expert consultations** with more than 20 ecosystem stakeholders to explore sandbox models, governance structures and risk-management approaches tailored to India.
- **Global benchmarking** of sandbox initiatives to compare structural design, regulatory integration and innovation-enabling mechanisms in different countries.

During these interactions, the participants or respondents voiced the need to create an ecosystem of AI sandboxes, not only as a means of establishing regulatory certainty but also to institute structured pathways for promoting the AI start-ups on their techno-commercial journeys.

↓ **Caption:** Visuals from a workshop with AI start-ups held in Bengaluru, Karnataka

2 Enablers of AI innovation in India

India can harness the AI opportunity through innovation by leveraging its core strengths outlined in Section 1.1. However, a few enablers need to be put in place for this to happen.

The World Economic Forum held consultations with Indian AI start-ups as well as industry leaders and policy-makers in workshops and one-on-one interviews to identify the basic enablers of AI innovation in India. These consultations focused particularly on priority sectors such as agriculture, healthcare, education and MSMEs. The findings can be broadly grouped into five categories.

Data enablers: AI start-ups often lack access to the local, AI-ready datasets that are crucial for building models and applications suited to the Indian context. The availability of recent and real-time data enhances efficiency and accuracy in model training and validation. The addition of vernacular-language datasets enhances local relevance, while clear governance frameworks on privacy and data sharing further smooth the path by increasing compliance and trust. Ease of access to real-world (anonymized) data would also accelerate the development of these datasets.

Data quality and local data (not translated content) through good governance practices would eliminate bias due to Western ethnicities and create models that suit the local population. Together, this set is referred to as data enablers: availability, access, data quality, local content, data governance, data protection.

Data access is a challenge across sectors – start-ups often lack high-quality, real-time and vernacular datasets, and data-sharing mechanisms among the systems of government, industry, academia and start-ups remain limited.

Fabian Bigar, Secretary-General, Ministry of Digital, Government of Malaysia

Computational infrastructure: Access to affordable, scalable compute capability enables the training of sophisticated AI models. The IndiaAI Mission initiative's initial aim of providing more than 18,000 graphics processing units (GPUs)[13] at subsidized rates to start-ups has been significant in addressing this challenge. In fact, this was increased to 34,000 GPUs as of June 2025 and several AI start-ups have been onboarded. Further, more kinds of publicly available and accessible compute infrastructure, such as DPI-enabled clusters, could enable and democratize AI experimentation.

AI sandboxes can act as launchpads for entirely new use cases by enabling developers, start-ups and researchers to safely test and refine cutting-edge solutions. From precision agriculture and AI-assisted diagnostics to intelligent public service delivery, these environments can accelerate the transition from promising ideas to scalable applications with real impact across India.

Shankar Maruwada, Co-Founder and Chief Executive Officer, EkStep Foundation

Model availability and contextual representation: The reliance on AI models trained on non-Indian data significantly increases costs and latency, with many lacking robust vernacular capabilities, restricting their applicability and effectiveness in addressing local market needs. Most are trained primarily on English-language data[14] (for example, OpenAI's GPT-3 uses ~92.7% English-language sources), limiting their performance and fairness in Indian contexts and introducing bias when deployed locally. Focusing on models trained on Indian content/languages is a great enabler.

Latency remains a significant challenge. Establishing an AI sandbox environment in India – with either indigenous models or direct integration of global models – can substantially reduce latency and enhance performance.

Keshav Reddy, Founder and Chief Executive Officer, Equal

Regulatory certainty and validation pathways: The creation of standardized validation frameworks and sector-specific regulatory benchmarks, along with a clear strategic direction on regulations and certification mechanisms, accelerates innovation. The regulatory enabler category is perhaps the strongest case for the AI sandbox.

> **In critical sectors such as healthcare and BFSI, the lack of awareness around standard validation frameworks makes it hard for start-ups to demonstrate compliance and safety – AI sandboxes, supported by expertise in AI risks and domain-specific regulations, can provide the testing environments needed to bridge this trust gap.**
>
> Sivaramakrishnan R. Guruvayur, Senior Research Fellow, Centre for Responsible AI (CeRAI), Indian Institute of Technology, Madras

Market access enabler: Start-ups can reach break-even sooner if they can start monetizing AI solutions effectively.[15] Access to early-stage, patient capital for deep tech must be promoted. In addition, structured mentorship and peer collaboration opportunities need to be structured. Preferential market access to the public sector for the solutions that pass the validation process in the AI sandbox can be a great incentive.

> **If you ask early-stage start-ups what problem they're solving or who they're selling to, the answers are often unclear. That's where mentoring and structured support – enabled through an AI sandbox ecosystem – can make a real difference.**
>
> Pradeep Jhunjhunwala, Head of Partner and Customer Success, Amazon Web Services

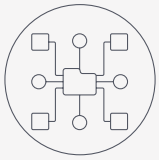
3 Creating enablers through AI sandboxes

Existing AI sandboxes around the world have been instrumental in creating one or more of the enablers specified in the previous section.

AI sandboxes can create one or more of the five AI enablers for AI start-ups and solution developers.

The focus areas of AI sandboxes in Table 1 broadly fall in two categories – **AI enablers** and **AI guardrails**.

TABLE 1 **Examples of AI sandboxes enabling AI innovation**

Challenge	Sandbox	Country	Enablers put in place by the sandbox
Data accessibility and governance 	FCA Digital Sandbox	United Kingdom	Offers access to 300+ GDPR-compliant datasets and more than 1,000 application programming interface (API) endpoints
	AI Hub	South Korea	Provides AI-ready datasets in 14 sectors including healthcare, finance and transportation
	NATO Data Science and AI Sandbox	International (NATO)	Grants access to classified NATO datasets in a secure sandbox environment
Computational infrastructure 	MITRE's Federal AI Sandbox	United States	Enables AI research and development (R&D) with 248 NVIDIA H100 GPUs for secure government-related experimentation
	NAIRR Pilot	United States	Offers compute capacity and infrastructure access to innovators via application-based approvals
	AI Trailblazers Sandbox	Singapore	Provides free access to Google Cloud's high-performance GPU infrastructure for GenAI prototyping

Challenge	Sandbox	Country	Enablers put in place by the Sandbox
Models and contextual representation	Harvard University AI Sandbox	United States	Centralizes access to large language models (LLMs) from OpenAI, Anthropic, Google and Meta in a secure interface
	MSBA AI Sandbox	United States	Offers LLM-based tools to explore generative AI (GenAI) in the legal domain
	AFRL GenAI Sandbox	United States (DoD)	Provides Air Force personnel with secure LLM access for AI experimentation
Validation and certification pathways	IMDA GenAI Evaluation Sandbox	Singapore	Features a standardized evaluation catalogue for LLM and GenAI product assessment
	Norway's Regulatory Sandbox	Norway	Supports solution validation in line with regulations and helps conduct data protection assessments
	NayaOne AI Sandbox	United Kingdom	Offers tools for model validation, robustness testing and AI governance metrics
Innovation ecosystem enablement	NeLC AI Sandbox in Digital Learning	Saudi Arabia	Provides expert consultations, resources and support for AI in education
	Qatar's AI & XR Sandbox	Qatar	Delivers mentorship from AI architects and data scientists through structured sessions
	Malaysia's AI Sandbox	Malaysia	Supports AI training and capacity-building through collaboration with educators and experts

Source: World Economic Forum analysis

4 The framework for the AI sandbox ecosystem

The strategic and operational frameworks for AI sandboxes proposed in this section are designed to establish the AI enablers and AI guardrails.

Given the fast-evolving nature of AI technologies, the diversity of use cases and the varied risk landscapes, a one-size-fits-all approach to establishing sandbox(es) is neither feasible nor desirable. Instead, an ecosystem of sandboxes must be envisioned, with each sandbox tailored to its specific objectives, sectoral priorities and stakeholder needs. In other words, an ecosystem of AI sandboxes should evolve, preferably meeting common standards and protocols for portability of AI solutions and collaboration of resources.

4.1 Vision of the AI sandbox

A shared strategic vision is necessary to guide innovators, policy-makers, regulators and enablers in shaping AI development that is not only cutting-edge but also responsible and inclusive.

This vision should serve as the north star for institutional design, infrastructure investments and governance mechanisms – ensuring that all AI sandbox initiatives are aligned with national priorities and public interest.

This vision underpins the framework that follows – built to address structural barriers through coordinated interventions across data access, compute capability, model validation, regulatory alignment and ecosystem support.

Vision statement of the AI sandbox workstream within the AI for India 2030 initiative

> To establish an AI sandbox ecosystem that catalyses responsible innovation, enhances the ease of doing AI research and development, and positions India as a global leader in artificial intelligence by 2030.

4.2 **Strategic framework:** Guiding principles and structure

To translate this vision into actionable outcomes, a strategic framework has been developed through extensive stakeholder consultations, global benchmarking and the deliberations of the AI for India 2030 Expert Group. The framework responds to India's unique opportunity and challenge – to lead in AI innovation while ensuring responsible governance.

The framework reflects a dual imperative:

- **Promote innovation** by providing start-ups, researchers and institutions with access to critical infrastructure, datasets and safe testing environments.
- **Embed safeguards** through effective governance, regulatory alignment and risk-management protocols to ensure that AI development is responsible, ethical and aligned with societal values.

The framework is structured across five interdependent layers of the AI ecosystem: **Governance**, **Innovation**, **Models**, **Data** and **Infrastructure**. Each layer identifies a set of **enablers** – to support experimentation and growth – and **guardrails** – to ensure compliance, security and trustworthiness.

FIGURE 2 **Strategic framework for AI sandboxes**

1. Governance layer

Enablers
- Multistakeholder governance boards
- Clear eligibility and access protocols
- Integration with policy and regulatory sandbox

Guardrails
- Responsible AI risk management frameworks (e.g. NIST RMF)
- Legal and ethical oversight mechanisms
- Grievance redressal and audit mechanisms

3. Models layer

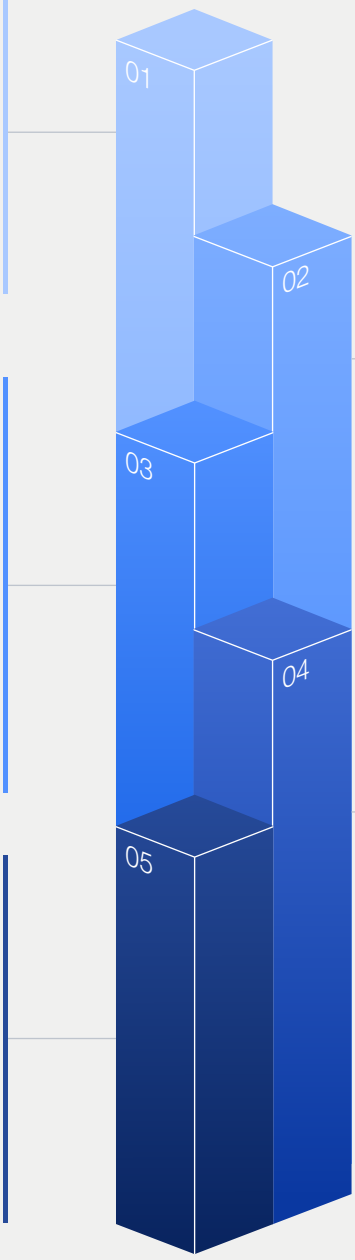
Enablers
- Development of localized small language models (SLMs)
- Localized and domain-specific model architectures
- Access to foundation models and application programming interfaces (APIs)

Guardrails
- Model evaluation benchmarks, laws and regulations
- Mandated use of local training data
- Disclosure of model parameters and fine-tuning methods

5. Infrastructure layer

Enablers
- Subsidized access to compute through public GPU clusters
- Preconfigured and secure dev-test environments
- PPP models for AI infrastructure

Guardrails
- Critical/zero-trust infrastructure security protocols
- Sectoral AI safety and security policies
- Guidelines on safe regulation



2. Innovation layer

Enablers
- Mentorship from domain experts on solution design
- Cross-functional, interdisciplinary teams
- Preferential market access for validated solutions

Guardrails
- Domain-specific validation frameworks for AI applications
- Trustworthiness and risk-evaluation protocols
- Deployment guardrails for high-risk use cases

4. Data layer

Enablers
- Access to multilingual, labelled, AI-ready datasets
- Federated or anonymized data-sharing models
- Data governance and consent frameworks

Guardrails
- Data-sharing protocols aligned with DEPA
- Anonymization and privacy standards and guidelines
- Compliance with data-protection legislation

Source: World Economic Forum analysis

The AI sandbox framework embodies the principle of "responsible innovation by design" as it is structured to support both innovation and regulation. Each layer within the framework plays a distinct role in enabling responsible, scalable AI innovation, as outlined below, starting with infrastructure at the base and working up:

Infrastructure: The infrastructure layer forms the technical backbone of the sandbox ecosystem. It ensures that start-ups and researchers can access the secure, affordable compute and development environments needed to build and test AI solutions. At the same time, it embeds safeguards such as secure access protocols and resilience standards to ensure that infrastructure is reliable, protected and ready to scale. The EU Act mandates the provision of all services free to SMEs and start-ups. The Government of India may take an appropriate view on what concessions can be extended to the SMEs and start-ups participating in the AI sandboxes.

Data: The data layer ensures access to high-quality, multilingual and AI-ready datasets that reflect India's diverse contexts. It enables experimentation through well-governed data access, including anonymized, labelled and federated sources. To build trust, this layer also enforces strict data-privacy standards, consent frameworks and compliance with the Digital Personal Data Protection (DPDP) Act[16] and emerging data protection regulations.

Models: The models layer supports the development of localized, domain-specific AI models that are representative of India's linguistic and cultural diversity. It enables access to pretrained models and tools for fine-tuning, allowing innovators to build contextually relevant solutions. Guardrails in this layer include evaluation standards for fairness, transparency and robustness to ensure that models are safe and reliable before deployment. A required precaution is the flagging of datasets/ content that are translated from English and originated outside India. This enables the models to avoid compounding the bias inherent in such datasets/content.

Innovation: The innovation layer focuses on translating AI capabilities into real-world use cases across sectors such as public safety, public health, healthcare, agriculture, education, finance, environment, climate action, sustainable energy, transportation, and public administration and public services. It enables innovators to pilot and refine solutions in controlled environments with access to curated data for training, validation and testing, and domain expertise for mentoring and early users. In parallel, India can also emerge as a leader in science-led innovation, where AI is accelerating discovery itself. Sandboxes can support this frontier through controlled experimentation in fields such as lab automation, simulation and autonomous scientific analysis. For instance, emerging systems such as *Robin* – a multi-agent AI platform capable of autonomously designing, executing and analysing scientific experiments – illustrate the kind of deep-tech applications that could benefit from sandbox support. Guardrails ensure that deployed applications meet sectoral standards, minimize risk and uphold public trust through validation and responsible deployment protocols.

Governance: The governance layer provides the overarching structure for coordination, accountability and risk management across the sandbox ecosystem. It enables multistakeholder participation, transparent decision-making and alignment with regulatory and ethical standards. Guardrails at this level ensure responsible oversight through structured governance boards, grievance redressal mechanisms and the application of risk management frameworks such as NIST RMF.

This layered and modular architecture ensures that AI innovation is pursued in a systemically safe, contextually relevant and future-ready manner. For instance, access to public compute infrastructure must be matched with enforceable security protocols, just as multilingual datasets must be governed by strong privacy and consent mechanisms.

By embedding both innovation drivers and ethical boundaries into every layer, the framework positions AI sandboxes not merely as experimental spaces but as trusted national platforms for safe, inclusive and scalable AI adoption. The following caveats are in order:

a. Not every instance of an AI sandbox needs to have all five layers, depending on the sector and the implementation model. For instance, for an AI sandbox dealing only in use cases not involving any personal or sensitive data, the governance layer need not be present.

b. Likewise, not every layer requires equal emphasis.

Each instance of an AI sandbox needs to be designed on a case-to-case basis involving a multidisciplinary team, consisting of domain experts, IT and AI professionals, and security, privacy and legal experts, besides public administrators.

4.3 Operational framework: Translating strategy into action

While the strategic framework outlines the core building blocks and principles of AI sandboxes, their real-world impact depends on how these ideas are implemented. The operational framework translates strategy into practice – offering a step-by-step roadmap for designing, launching and scaling AI sandboxes tailored to India's context.

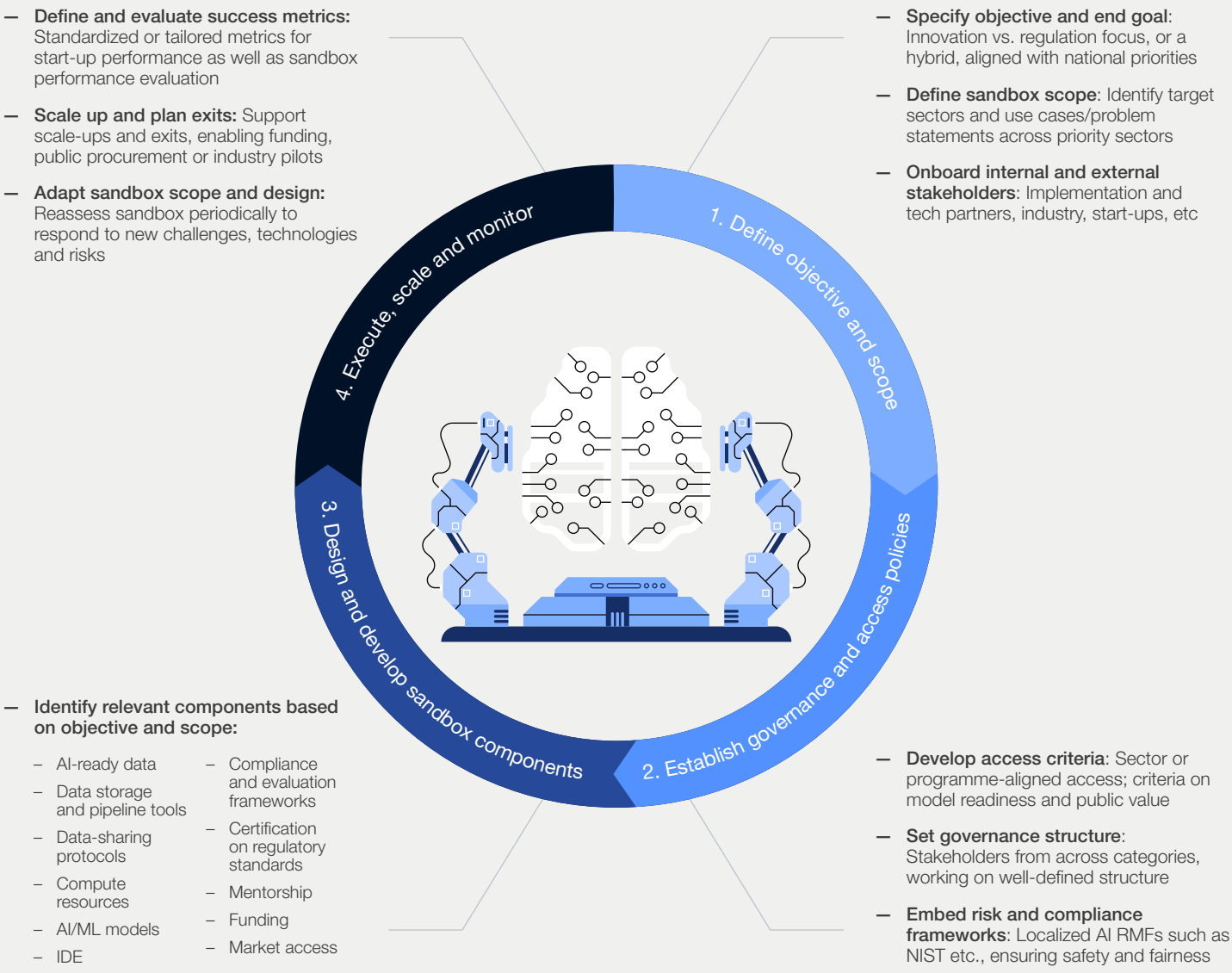
This section outlines four critical phases of operationalization:

1. Define the objectives and scope
2. Establish a governance body and access protocols
3. Design and develop sandbox components in alignment with the scope
4. Execute, scale and monitor

Each phase incorporates the enablers and guardrails described earlier, ensuring that sandboxes remain not only functional but also inclusive, trusted and aligned with India's innovation priorities. The caveats listed in Section 4.2 need be kept in mind.

This phased approach ensures that AI sandboxes evolve from short-term pilots into long-term national assets – supporting responsible innovation at scale while embedding measurable safeguards and outcomes.

FIGURE 3 **Operational framework for establishing an AI sandbox**



Source: World Economic Forum analysis

4.3.1 Define objectives and scope

To be effective, an AI sandbox must begin with a clearly defined objective – whether the focus is enabling innovation, regulatory experimentation or a hybrid approach.

- **Clearly articulate the primary purpose:** innovation, regulation or hybrid – along with specific end goals.
- **Identify the scope, based on target sectors and anchor use cases:** for example, healthcare diagnostics, MSME export compliance agents, agri-input optimization tools, voice-first AI agents for rural service delivery, autonomous agri-drones, Sewa agents (AI-based virtual assistants for accessing public schemes and entitlements) in rural India or AI-powered warehouse robots.
- **Map key stakeholders:** government nodal bodies (government agencies with primary responsibility for sectoral implementation and coordination), AI start-ups, domain experts and infrastructure providers and potential adopters (for example, public agencies).

Example: A sandbox for AI-enabled diagnostics would involve India's Central Drugs Standard Control Organization (CDSCO),[17] health departments, AI health-tech start-ups and medical institutions, enabling sector-aligned validation and deployment.

4.3.2 Establish multistakeholder governance and access policies

A strong governance model builds credibility and ensures trust in experimentation environments, which is essential for secure, transparent and inclusive AI sandbox environments. For research-intensive sectors, participation also depends on robust IP protection and clear data-ownership norms. Sandboxes must support sector-specific agreements, enable confidential computing environments and maintain audit trails to safeguard proprietary research and sensitive workflows.

This can be enabled by the following:

- **Define access and participation/eligibility criteria** based on alignment with sectoral needs or problem statements. Ensure selection criteria are transparent and accessible, minimizing bureaucratic hurdles such as excessive paperwork. A single-window entry system with modules linked to relevant government schemes (e.g. Startup India, India AI Mission) can further ease participation.
- **Set up inclusive governance boards** with representation from ministries, legal and policy experts in AI policy and AI risk management, start-ups, industry, academia and civil society.
- **Embed a localized responsible AI risk-management framework**, adapted from global standards such as the US government's National Institute of Standards and Technology (NIST) AI Risk Management Framework (RMF),[18] to systematically identify, document and manage AI risks.
- **Enable clear coordination protocols** for onboarding, stakeholder management and conflict resolution. Inclusion of consumer consent mechanisms, where applicable, can improve trust, scale and innovation.
- **Incorporate robust data-sharing and privacy policies**, modelled on frameworks such as India's Data Empowerment and Protection Architecture (DEPA).[19]
- To enable secure multi-tenant data access, **adopt security approaches** such as Zero Trust architecture and confidential computing. Include protocols for secure data destruction post-usage, especially for sensitive sectors such as healthcare.

Example: In an education sandbox, the inclusion of edtech firms, relevant state departments and the State Councils of Educational Research and Training (SCERTs) would ensure that solutions are aligned with ground-level educational needs and policy pathways.

4.3.3 Design and develop core AI sandbox components

To effectively support AI experimentation and deployment, sandboxes must be built around core components that address real-world constraints faced by Indian start-ups. These components fall under three main categories:

1. **Data and infrastructure enablers**

- **Provide AI-ready localized and multilingual datasets** through secure data pipelines and data-sharing protocols, including federated systems or data clean rooms, enabling trusted, multi-tenant collaboration.
- **Support vernacular speech datasets** and automatic speech recognition (ASR) models in vernacular languages to enable inclusive, voice-first AI agents for rural and semi-urban contexts. **Ensure data governance and discipline** aligned with India's emerging data economy principles.
- **Offer affordable access to compute infrastructure**, including shared access to GPU clusters and subsidized infrastructure models via public–private partnerships. Enable compute access to also support hybrid cloud and edge environments, **enabling scalable testing** of agentic and physical AI solutions in decentralized or bandwidth-constrained settings.
- **Provide access to foundational or pretrained AI/machine learning (ML) models**, including vernacular models developed through platforms such as Bhashini or the recently released Sarvam's model.
- **Offer preconfigured integrated development environments** for streamlined coding, model development and testing.

2. **Trust and validation enablers**

- **Embed compliance and evaluation frameworks**, such as the NIST RMF, adapted to Indian sectoral and regional requirements for fairness, safety and explicability.
- **Enable certification or precertification support** aligned to sectoral regulatory standards to facilitate deployment, such as the Insurance Regulation and Development Authority of India (IRDAI)[20] for insurance or the Reserve Bank of India (RBI)[21] for banking and finance.
- **Provide automated tools for benchmarking, model validation and performance testing** to ensure fairness, robustness and safety before full-scale deployment. All sandbox participants may be encouraged to publish reports on bias mitigation, citizen protection and safety frameworks. Differential privacy techniques, where appropriate, should also be considered in sandbox data-handling protocols.

3. **Ecosystem enablers**

- **Offer incentive programmes** such as milestone-based funding, innovation grants and pilot challenges to incentivize high-impact solutions.
- **Create structured mentorship networks** involving policy-makers, tech original equipment manufacturers (OEMs), domain experts, industry stakeholders, start-ups, researchers, technical experts and adopters to support solution readiness and scaling. A pool of experts comprising industry professionals and academics may be curated to guide participants throughout the sandbox life cycle and aid in transitioning viable projects to scale.
- **Facilitate market access** through integration with public platforms (such as AI-based Sewa agents for citizen services in vernacular languages) and establish clear commercialization pathways linking validated solutions to government procurement, market integrations or seed-stage investor showcases.

Example: A sandbox hosted in collaboration with IRDAI could enable start-ups to test agentic AI for insurance underwriting, evaluate bias and performance, and enable emerging models such as AI-based risk insurance.[22]

4.3.4 Execute in phases, scale and monitor outcomes

AI sandboxes should be implemented in an agile, phased manner – starting small, learning from early experiments and scaling up with robust measurement and feedback loops. This approach helps mitigate risk, optimize resources and enable more targeted interventions. The main steps for operational execution are as follows:

- **Begin with a minimal viable pilot** – focused either on one sector or on cross-sector use cases where dependencies exist (e.g. open-source finance in BFSI) – **or a defined geographical region**, to test feasibility, stakeholder engagement and operational workflows.

- **Define clear key performance indicators (KPIs)** covering participation, performance, model validation, regulatory feedback and adoption rates. Examples include the following:
  - Number of start-ups supported
  - Number of validated models and certifications issued
  - Number of patents filed and commercial partnerships formed
  - Deployment outcomes such as “1 million agent deployments/month” or “vernacular agents piloted across 100+ districts”
- **Iterate continuously based on structured feedback** to refine scope, eligibility, operational design, sandbox components and support systems. Periodic reviews should assess technological, regulatory and commercial outcomes. Tracking mechanisms must be backed by adequately resourced teams in government agencies to translate sandbox learnings into timely policy or regulatory updates.
- **Support structured exits** and scale-ups, including integration into national programmes through public procurement, innovation grants, VC matchmaking or regulatory endorsement. Enable mentorship from policy-makers, tech OEMs and academic experts to support start-up readiness for broader deployment.

Example: A sandbox focused on agentic AI in agriculture could track adoption with use cases tested by farmer producer organizations (FPOs) or agritech platforms. Based on successful outcomes, validated solutions could be transitioned to the Ministry of Agriculture or relevant state departments for large-scale adoption and policy integration.

The strategic and operational frameworks presented here offer a structured approach to enabling responsible AI innovation at scale. By embedding both enablers and guardrails across the AI value chain – from infrastructure and data to applications and governance – the framework ensures that innovation is pursued in a safe, inclusive and contextually grounded manner on an end-to-end basis. The accompanying operational roadmap provides a phased path for implementation, grounded in real-world constraints and sectoral needs.

5 A call to action

AI sandboxes become a meaningful lever for India's AI ecosystem through coordinated action by all major stakeholder groups.

As India seeks to position itself as a global AI powerhouse, the establishment of AI sandboxes becomes critical to accelerating responsible and inclusive AI innovation.

The following actions outline the roles and responsibilities of major stakeholders in establishing AI sandboxes across the country.

Government and policy-makers:

- Encourage the launch of a few AI sandboxes – at the national level and one or more state-level, sector-specific initiatives – within a 12–14-month horizon, focused on priority areas identified in this paper. States may consider selecting distinct sectors aligned with their economic priorities to avoid duplication and ensure depth of experimentation. This approach can help optimize expert resources and foster a diverse portfolio of pilots across the country.
- Promote AI sandbox pilots through national programmes such as the IndiaAI Mission or DPI efforts. It is essential to ensure the benefits of sandbox-led AI innovation reach citizens. Government agencies and sandbox designs should prioritize accessibility and inclusion to maximize public value.
- Develop model AI sandbox policies and data-sharing protocols in collaboration with NITI Aayog, MeitY and state governments.
- Invest in DPI for AI – including compute and AI-ready datasets – to reduce the cost of innovation and incentivize the creation of vernacular datasets and language tools.
- Appoint a nodal agency (such as Digital India Corporation) to standardize sandbox governance and coordinate between central and state deployments. Facilitate a national registry of AI sandboxes to promote interoperability, documentation of learnings and cross-sector knowledge transfer.
- Consider creating a pool of experts by calling upon industry experts and academicians to provide tactical guidance and support to participants throughout the sandbox life cycle and during the transition to scaling post cessation of the sandbox.
- Establish formal feedback mechanisms to integrate sandbox learnings into national AI strategy, regulatory frameworks and sectoral standards.

– Develop structured pathways for sandbox graduation, including public procurement, DPI integration and access to patient capital for scale-up.

– Explore formulating a policy on preferential market access to promote start-ups that have had their solutions and value proposition validated successfully at one of the sandboxes, within limits permitted by GFR.

Industry and technology partners:

– Contribute cloud credits, LLM APIs and compute resources through corporate social responsibility (CSR) or partnership models (such as investing in compute infrastructure annually for each sandbox).

– Establish mentorship and evaluation partnerships through industry consortia to guide start-ups on product validation, ethics and deployment readiness.

– Support market access pathways by running joint innovation challenges or offering fast-track procurement for sandbox graduates.

Academia and research institutions:

– Host regulatory-aligned evaluation cells within universities to certify AI solutions (especially in high-stakes sectors such as health and education).

– Participate in mentorship programmes for start-ups, engage with sandbox governance boards and lead capacity-building for domain-specific model validation.

– Document and publish case studies of sandbox experiments to contribute to global learning and policy insights.

– Promote and support AI-led scientific discovery by participating in sandbox pilots focused on lab simulation, autonomous experimentation and deep-tech research workflows.

Start-ups and innovators:

– Actively engage in sandbox pilots that align with their product–market fit and domain strengths.

– Offer data and feedback loops to sandbox governance boards and regulators to improve sandbox model and policy design.

– Collaborate with regulators and adopters to co-develop deployment and scale-up plans.

– Integrate user feedback and community perspectives into solution design and sandbox evaluation, particularly in public-facing sectors. Institutionalizing these feedback loops through formal channels can help shape agile, evidence-based regulation and AI policy frameworks.

Conclusion

India can be a model for the world in developing AI suited to local needs.

India has a unique opportunity to lead the next phase of AI innovation by building solutions that are inclusive, contextually grounded and scalable. With its strong DPI, dynamic start-up ecosystem and growing technical capacity, the country is well placed to develop AI that addresses local needs while setting global benchmarks.

This paper presents a practical roadmap for operationalizing AI sandboxes in India, drawing on extensive stakeholder consultations, global benchmarking and expert input. These sandboxes are not merely testing environments – they can serve as catalysts for innovation, validation and deployment of AI solutions across priority sectors such as agriculture, healthcare and MSMEs.

The strategic and operational frameworks outlined here embed both enablers and guardrails throughout the AI value chain. AI sandboxes can support responsible innovation while building public trust and ensuring regulatory alignment, representing responsible AI by design.

Realizing this vision will require sustained collaboration across government, industry, academia and start-ups. With structured governance, transparent evaluation and continuous feedback, AI sandboxes can evolve into long-term infrastructure for innovation.

Over time, these sandboxes can also inform policy, shape national standards and unlock commercialization pathways – positioning India not only as an early adopter but also as a global leader in inclusive and trusted AI development. As emerging economies look to India for inspiration, the sandbox model can serve as a blueprint for scaling responsible AI globally.

Appendix

BOX **Institutional models for AI sandbox governance**

A review of AI sandboxes established globally highlights the diverse objectives they serve. These objectives are often shaped by the mandate and priorities of the organization leading the sandbox. Building a comprehensive AI ecosystem requires the coordinated efforts of multiple sandboxes, each led by a different type of institution – government bodies, industry regulators, industry bodies, academia or private organizations – addressing distinct aspects of the broader challenge. The table below outlines the main categories of sandbox-leading organizations and their typical objectives.

Typical sandbox objective across stakeholders		Global AI sandbox examples			
Leading stakeholder	Typical objective	Organization name	Sandbox name	Sandbox components	Key purpose
Government	Support the development of a robust AI ecosystem by enabling innovation through access to compute and mentorship, accelerating adoption through capability-building efforts and offering regulatory support	Danish Data Protection Agency, Denmark	Regulatory Sandbox for AI	Regulation guidance and expertise	Support AI innovation by providing guidance on regulatory requirements
		Ministry of the Economy and Innovation of the Republic of Lithuania, Lithuania	AI Sandbox	Regulatory assessment, compliance certification	Space for businesses to safely test innovations and ensure regulatory compliance
		Infocomm Media Development Authority, Singapore	GenAI Evaluation Sandbox	Testing and validation, regulatory evaluation	Support safe and trustworthy AI development and adoption
		Malaysian Research Accelerator for Technology and Innovation, Malaysia	AI Sandbox	Compute, datasets, testing and validation, capability-building, mentorship	Boost the adoption of AI throughout Malaysian organizations
		Ministry of Communication and Information Technology, State of Qatar	AI Sandbox	Integrated development environment (IDE), testing and validation, mentorship, capability-building	Flexible environment for developers, innovators and businesses to experiment with and develop AI-driven solutions
Industry regulator	Address regulatory challenges, support risk mitigation and enable compliant AI adoption in regulated sectors	Medicines and Healthcare Products Regulatory Agency, United Kingdom	AI Airlock	Regulatory evaluation, mentorship	Identify regulatory challenges to AI as a medical device (AIaMD) and work collaboratively to understand and potentially mitigate risks
		Financial Conduct Authority, United Kingdom	Digital Sandbox	Datasets, IDE, mentorship, market access	Facilitate the development and launch of cutting-edge solutions within the financial services industry

Industry body	Enable sector-specific innovation and responsible use of AI	Minnesota State Bar Association, USA	AI Sandbox	IDE, LLMs, regulatory evaluation	Controlled environment for organizations to use LLMs to help improve access to justice
		National eLearning Center, Saudi Arabia	AI Sandbox in Digital Learning	Datasets, mentorship, funding	Accelerate innovation and adoption of AI solutions in learning
Academia	Promote experimentation, foundational research and skill development through secure access to AI infrastructure	Harvard University, USA	Harvard AI Sandbox	LLMs, data analysis and visualization, code execution, IDE	Secure environment to experiment with GenAI
		Princeton University, USA	Princeton AI Sandbox	Compute, LLMs	Secure environment for researchers with access to multiple LLMs
		Cornell University, USA	Cornell SandboxAI	Compute, LLMs, data analysis and visualization	Put Cornell at the forefront of AI innovation by providing faculty and staff with access to AI tools
		Charles University, USA	Cuni AI Sandbox	Compute, LLMs, IDE	Access to advanced GenAI models and security risks mitigation
		Stanford University, USA	Stanford AI Playground	LLMs, IDE	User-friendly platform for Stanford faculty, staff and students to safely try AI models
Private/non-government	Accelerate AI product development, testing and scale-up through secure infrastructure and industry collaboration	NayaOne, United Kingdom	NayaOne AI Sandbox	IDE, datasets, testing and validation	Empower financial institutions to launch AI products rapidly and securely
		MITRE Corporation, USA	MITRE's Federal AI Sandbox	Compute, mentorship	Accelerate AI research and development for government applications

Contributors

World Economic Forum

Satyanarayana Jeedigunta
Chief Advisor, Centre for the Fourth Industrial Revolution India

Purushottam Kaushik
Head, Centre for the Fourth Industrial Revolution India

Ayushi Sarna
Specialist, Data Policy and Artificial Intelligence, Centre for the Fourth Industrial Revolution India

Harsh Sharma
Lead, AI and ML, Centre for the Fourth Industrial Revolution India

Sakshi Vohra
Strategy and Operations Specialist, Centre for the Fourth Industrial Revolution India

BCG X

Saumil Agarwal
World Economic Forum Project Fellow, BCG

Dipayan Chakraborty
Partner and Vice-President Data Science, BCG X

Gaurav Jindal
Managing Director and Partner, BCG X

Nipun Kalra
Managing Director, Senior Partner and India Head, BCG X

Sambhav Kela
World Economic Forum Project Fellow, BCG

Pooja Rajdev
Principal, BCG X

Acknowledgements

AI for India 2030 Advisory Council

Council Members

S. Krishnan
Council Co-Chair; Secretary, Ministry of Electronics and IT (MeitY)

Ajay Sood
Council Co-Chair; Principal Scientific Adviser to the Government of India

Rajiv Bansal
Chief Executive Officer, NISG

T.P. Chopra
President and Chief Executive Officer, BLP

Vishal Dhupar
Managing Director – India and South Asia, Nvidia

Sindhu Gangadharan
Senior Vice-President, SAP

Debjani Ghosh
Distinguished Fellow, NITI Aayog

Vijay Guntur
Chief Technology Officer, HCLTech

Mohit Kapoor
Group Chief Technology Officer, Mahindra Group

Abhay Karandikar
Secretary, Department of Science and Technology

Ekroop Kaur
Secretary, Department of Electronics and Information Technology, Government of Karnataka

Sanjeev Krishan
Chairperson, PwC India

Shailesh Kumar
Chief Data Scientist, Centre of Excellence AI/ML, RIL

Balaraman Ravindran
Head, Centre for Responsible AI, IIT Madras

Sharad Sharma
Co-Founder, iSPIRT

Romal Shetty
Chief Executive Officer, Deloitte – India

Abhishek Singh
Additional Secretary (MeitY)

Shekar Sivasubramanian
Chief Executive Officer, Wadhwani AI

Rohini Srivathsa
Chief Technology Officer,
Microsoft India and South Asia

Rafee Tarafdar
Chief Technology Officer, Infosys

Special Invitees

Pratyush Kumar
Co-Founder, Sarvam

Jayesh Ranjan
Special Chief Secretary, Government of Telangana

Munish Sharda
Executive Director, Axis Bank

Santosh Viswanathan
Vice-President and Managing Director,
India Region, Intel

Co-Hosts

Preeti Banzal
Adviser/Scientist "G", Office of the Principal Scientific Adviser

Kavita Bhatia
Chief Operating Officer, IndiaAI, Ministry of Electronics and IT (MeitY)

Sangeeta Gupta
Senior Vice-President and Chief Strategy Officer, Nasscom

Expert Group AI Sandbox

Ekroop Kaur
Chairperson; Secretary, Department of Electronics and Information Technology, Government of Karnataka

Shruti Agrawal
Head, Conversation AI, Sarvam

Ibrahim Abdullah AlShunaifi
Internet of Things (IoT) Lead, Centre for the Fourth Industrial Revolution, Saudi Arabia

Kavita Bhatia
Chief Operating Officer, IndiaAI, Ministry of Electronics and IT (MeitY)

Fabian Bigar
Secretary General, Ministry of Digital, Malaysia

Ankit Bose
Head of Nasscom AI, Nasscom

Achyut Chandra
Group Manager and Lead, GovTech Strategy and Open Innovation, HCLSoftware

Rakesh Dubbudu
Founder and Chief Executive Officer, Factly (Dataful)

Shruti Garg
Strategic Partnerships Manager, Google Research

Zvika Goltzman
Acting Vice-President, Israel Innovation Authority

Sivaramakrishnan R. Guruvayur
Senior Research Fellow, Centre for Responsible AI (CeRAI), IIT Madras

Pradeep Jhunjhunwala
Head of Partner and Customer Success,
Amazon Web Services

Rama Devi Lanka
Officer on Special Duty, Emerging Technologies Wing, Government of Telangana

Ranjani Mani
Director and Country Head, Generative AI,
Microsoft India and South Asia

Shankar Maruwada
Co-Founder and Chief Executive Officer,
EkStep Foundation

Ramesh Padala
Managing Director, BCG X

Sharad Sharma
Co-Founder, iSPIRT Foundation

Aakrit Vaish
Advisor, IndiaAI Mission

Kiran Gopal Vaska
Joint Secretary, National Health Authority (India)

World Economic Forum

Karla Yee Amezaga
Lead, Data Policy

Abhishek Balakrishnan
Lead, AI and Innovation

Maria Basso
Head, AI Application and Impact

Benjamin Cedric Larsen
Lead, AI and ML

Special mentions:

Cropin

Equal

Giftolexia

Haptik

LEAD School

NxtWave

Nurix AI

Sarvam

String Bio

Production

Bianca Gay-Fulconis
Designer, 1-Pact Edition

Tanya Korniichuk
Illustrator, 1-Pact Edition

Alison Moore
Editor, Astra Content

Endnotes

1. World Economic Forum. (2019, October 23). *Navigating uncharted waters: A roadmap to responsible innovation with AI in financial services*. https://www.weforum.org/publications/navigating-uncharted-waters-a-roadmap-to-responsible-innovation-with-ai-in-financial-services/
2. World Economic Forum. (2025). *Future farming in India: A playbook for scaling artificial intelligence in agriculture.* https://www.weforum.org/publications/future-farming-a-playbook-for-scaling-artificial-intelligence-in-agriculture/
3. Pounds, E. (2024, October 22). *What is agentic AI?* NVIDIA. https://blogs.nvidia.com/blog/what-is-agentic-ai/
4. Mucci, T., & Stryker, C. (2023, December 18). *What is artificial superintelligence?* IBM. https://www.ibm.com/think/topics/artificial-superintelligence
5. EUR-Lex. (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689
6. Datasphere Initiative. (2025). *Sandboxes for AI: Tools for a new frontier*. https://www.thedatasphere.org/wp-content/uploads/2025/02/Report-Sandboxes-for-AI-2025.pdf
7. Datatilsynet. (n.d.). *Regulatory privacy sandbox.* Retrieved May 8, 2025, from https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/
8. Ministry of Science, Technology and Innovation. (2024, April 18). *The launching of artificial intelligence (AI) sandbox programme together with NVIDIA.* https://sandbox.gov.my/events/the-launching-of-artificial-intelligence-ai-sandbox-programme-together-with-nvidia
9. Brazilian Data Protection Authority. (2023, October 3). *ANPD's call for contributions to the regulatory sandbox for artificial intelligence and data protection in Brazil is now open.* https://www.gov.br/anpd/pt-br/assuntos/noticias/anpds-call-for-contributions-to-the-regulatory-sandbox-for-artificial-intelligence-and-data-protection-in-brazil-is-now-open
10. Infocomm Media Development Authority. (2023, October 31). *First of its kind generative AI evaluation sandbox for trusted AI by AI Verify Foundation and IMDA* [Press release]. https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/generative-ai-evaluation-sandbox
11. Information Commissioner's Office. (n.d.). *Regulatory sandbox.* Retrieved May 8, 2025, from https://ico.org.uk/sandbox
12. European Commission. (2022, June 8). *Launch event for the Spanish regulatory sandbox on artificial intelligence.* https://digital-strategy.ec.europa.eu/en/events/launch-event-spanish-regulatory-sandbox-artificial-intelligence#:~:text=The%20Spanish%20Secretary%20of%20State,for%20Spain%20and%20for%20Europe
13. IndiaAI. (n.d.). *India AI compute capacity.* Retrieved June 26, 2025, from https://indiaai.gov.in/hub/indiaai-compute-capacity
14. Xu, Y., Hu, L., Zhao, J., Qiu, Z., Ye, Y., & Gu, H. (2024). *A survey on multilingual large language models: Corpora, Alignment, and Bias.* arXiv. https://arxiv.org/html/2404.00929v1#:~:text=GPT,Text%20prompts%20written
15. The Economic Times. (2025, April 6). *ChatGPT downloads surge in India, but revenue lags behind: Report.* https://economictimes.indiatimes.com/tech/artificial-intelligence/chatgpt-downloads-surge-in-india-but-revenue-lags-behind-report/articleshow/120039540.cms?from=mdr
16. Ministry of Law and Justice. (2023, August 11). *The Digital Personal Data Protection Act, 2023.* The Gazette of India. https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf
17. Central Drugs Standard Control Organization. (n.d.). *Home.* Ministry of Health & Family Welfare, Government of India. Retrieved May 24, 2025, from https://cdsco.gov.in/opencms/opencms/en/Home/
18. Tabassi, E. (2023). *Artificial intelligence risk management framework (AI RMF 1.0).* United States National Institute of Standards and Technology. https://www.nist.gov/itl/ai-risk-management-framework
19. NITI Aayog. (2020, August). *Data empowerment and protection architecture: A secure consent-based data sharing framework to accelerate financial inclusion – Draft for discussion.* https://www.niti.gov.in/sites/default/files/2023-03/Data-Empowerment-and-Protection-Architecture-A-Secure-Consent-Based.pdf
20. Insurance Regulatory and Development Authority of India. (n.d.). *Home.* Ministry of Finance, Government of India. Retrieved May 24, 2025, from https://irdai.gov.in/
21. Reserve Bank of India. (n.d.). *Home.* Retrieved May 24, 2025, from https://www.rbi.org.in/
22. Schmelzer, R. (2025, April 30). *AI gone wrong? Now there's insurance for that.* Forbes. https://www.forbes.com/sites/ronschmelzer/2025/04/30/ai-gone-wrong-now-theres-insurance-for-that/

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org