

# Regulatory Sandbox for Responsible AI

\*\*\*\*\*\*\*\*\*\*

### Acknowledgement

Chase would like to acknowledge and thank Anup Wadhawan, Former Secretary, Government of India & Senior Fellow, The Indian School of Public Policy (ISPP), Ashutosh Chadha, Director and Country Head Government Affairs & Public Policy, Microsoft, Atul Kumar, Lead- Government Initiatives, Data Security Council of India (DSCI), Dr. Avik Sarkar, Senior Research Consultant & Visiting Faculty, Indian School of Business, Bharat Chugh, Lawyer, Founder, The Chambers of Bharat Chugh, Jhalak Kakkar, Executive Director, Centre for Communication Governance, NLU Delhi (CCG), NLU Delhi, Manojkumar Parmar, Founder, CEO, CTO, AlShield, Dr Pankaj Dikshit, Chief Technology Officer, Government e-Marketplace (GeM), Rajat Khaturia, Dean & Professor, Shiv Nadar University (SNU), Senior Visiting Professor, Indian Council for Research on International Economic Relations (ICRIER), Tariq Musthafa, Principal, Omidyar Network India, Venkatesh Krishnamoorthy, Country Manager — India, BSA, Vinay Kumar Sankarapu, Founder and CEO, Arya.ai, Aditya Nayan, Associate Director - Partnerships and Fundraising, Wahwani AI for their valuable inputs to the paper and the roundtable discussion.



### **Executive Summary**

India is fast emerging as a leader in technology as it is a hub of skilled human resources, an market ripe for expansion and supported by futuristic laws and policies. Technologies such as Artificial Intelligence (AI) are in the initial stages of development, capable of yielding a wide range of socio-economic benefits across economic sectors. With its vast population, varied data sets and focus on Digital Public Infrastructure India can take the lead in developing and training successful AI models for the world. India's futuristic upcoming laws and policies with a focus on building a responsible AI ecosystem puts it in the lead of becoming a global leader in responsible AI. India's leadership in GPAI and the upcoming AI summit hold immense potential for it to take the lead in building a governance framework for responsible AI, both for itself and the Global South.

A governance framework for responsible AI needs to address several challenges such as inter-play between sectoral regulators, transnational nature, accountability, transparency, protecting privacy, understanding black-box and bias. The G20 New Delhi Declaration it highlighted the need for a pro-innovation regulatory/ governance approach that maximizes the benefits and takes into account the risks associated with the use of AI. The primary goal for any regulation, especially for an emerging areas such as AI, should be to foster the development of new technology, concurrently with the mitigation of potential harms. To achieve this balance, it is necessary to implement innovative regulatory approaches, such as sandboxing.

Regulatory sandboxes are emerging as an effective way of regulating new and emerging technology/concepts to promote responsible innovation. More and more countries and sectors within the country are adopting regulatory sandboxes for emerging tech from Web 3 to Al. In India, regulatory sandboxes have primarily been implemented within the fintech sector. However, some states have extended their use to explore emerging technologies such as blockchain, Web 3, and Al -- beyond the confines of the fintech industry.

This paper conducts an analysis of the regulatory sandboxes established in India (refer to Annexure-2) as well as those in other countries and multilateral organizations (refer to Annexure-1). This examination was followed by extensive interaction with AI experts from industry, academia, start-ups, government, and multilateral agencies. Based on these learnings, we have arrived at the following considerations for designing the regulatory sandbox for AI. These have been explained in detail in this report.







### **Post-sandbox**



The recommendations were supplemented with the discussions during the roundtable and comments received post the deliberations.

### India's Opportunity & Challenges in Al

Emerging technologies like AI have become focal points of extensive policy discussions and initiatives today. AI is still in its early stages of development but holds the potential to deliver a broad spectrum of socio-economic advantages across industry sectors. AI has the capacity to unlock numerous latent opportunities within India. A few are detailed below:

#### **Economic Growth**

In recent years, India has witnessed a swift expansion of its economy, with a pivotal driver being the integration of contemporary technologies. The adoption of these advanced technologies by businesses has resulted in increased productivity and efficiency, consequently yielding increased profits and a surge in job creation. The utilization of modern technologies frequently catalyzes the emergence of novel industries and markets, amplifying prospects for economic expansion.

#### Rebranding

India has long branded itself as the world's leading outsourcing destination for global companies. In 2019, its outsourcing industry was evaluated at \$150 billion<sup>1</sup>. Proactive engagement with new technologies and regulations encouraging innovation can provide an opportunity and incentive to reinvent and rebrand itself as the hub of technological innovation. If favorable conditions are fostered, the country has the potential to develop its urban centers and promote the Silicon Valley spirit. It could also be in prime position to achieve global tech hub status given the presence of two tech savvy cities, namely Bengaluru in the south and Gurgaon in the north.

#### **Job Prospects**

In India, the adoption of the latest technology could give rise to millions of new jobs, especially in the IT industry. According to a 2022 NASSCOM report<sup>2</sup>, 60% of Indian Web3 startups were established overseas but employed domestic technical talent. Data provided by Indian Staffing Federation (ISF) on the IT staffing industry suggests a sharp growth of 30.7% in 2022 as opposed to 14.1% the year before. These demands are primarily driven by digital adoption in sectors such as fintech, IT, and infrastructure. Some domains where jobs can be generated have been mentioned here.

#### **Avenues of Job Creation**



https://economictimes.indiatimes.com/tech/ites/indias-technology-vendors-paddling-shaky-boats/articleshow/56543653.cms?from=mdr
 https://community.nasscom.in/communities/emerging-tech/impact-new-and-emerging-technology-economic-development-india

#### **Reduced Brain Drain**

Brain drain is the movement of skilled labor from one country to another, in search of job prospects and growth. It poses barriers for countries to achieve their sustainable economic development goals owing to reduced technological innovation and creation of fragile economies. In this context, as per a government survey conducted in 2017, it was seen that about 12% of scientist and 38% of doctors in the United States (US) are Indians. In NASA, 36% or 4 out of 10 scientists are Indians; 34% of employees at Microsoft, 28% at IBM, 17% at intel, 13% at XEROX and more than 12% at google are Indians. Recent data suggests that over 1.6 lakh Indians renounced their citizenship in 2021 and round 1.8 lakhs in 2022. Al, in conjunction with other emerging technologies, possesses the potential to significantly enhance both economic growth and employment opportunities. This heightens the likelihood of citizens securing employment while concurrently fostering an environment conducive to innovation and invention. Consequently, it can play a constructive role in mitigating the brain drain, as individuals are incentivized to contribute to their home country's technological advancements and economic prosperity.

#### **Global Technology Leader**

Tech is an area where there's great potential for India to become a global leader given its expertise, human resources and dynamic tech and start-up ecosystem. In order not to fall behind in the global competition for AI adoption, it is imperative to establish regulatory frameworks that are tailored to the complexities and nuances of emerging technologies within the Indian context The technology curve of India is increasing exponentially. Resilient and consistent efforts in policy and science have created fertile grounds for tech innovation and entrepreneurial growth. There is a conducive environment for the country to emerge as a leader in AI adoption. Some of the factors which can contribute towards the conduciveness of tech innovation and ease the process of technology uptake have been mentioned in the figure below<sup>3</sup>.



 https://www.wipo.int/edocs/pubdocs/en/wipo\_pub\_2000\_2022/in.pdf; https://www.investindia.gov.in/team-india-blogs/artificial-intelligence-poweringindias-growth-story; https://www.indiabudget.gov.in/economicsurvey/doc/eschapter/echap12.pdf; https://pib.gov.in/Pressreleaseshare.aspx?PRID=1863536



As seen above, harnessing, adopting and building a cohesive regulatory ecosystem presents multiple opportunities for India. At the same time, one should be cognizant of the risks associated and apprehended with AI regulation of high-risk AI. Society must be protected but without risking innovation. Al's regulation, however, is challenging owing to a range of factors enunciated below:



#### Pervasive and Non-Linear

Al is pervasive and non-linear. Its functioning is dependent on machines which make decisions based on the datasets they have been trained upon. For instance, self-driving cars communicate with smart transportation infrastructure; smart devices and algorithms, which respond to and predict humaninteractions. Further, Al embedded with products and services evolves quickly and shift from one regulatory category to another. For example, if Al is used for disease detection, it could fall under the jurisdiction of health regulators. If it expands into drone services, it will fall under the purview of aviation regulators. If Al is used in self-driving cars for passengers, it may come under the jurisdiction of the transport regulators. Maintaining consistency in regulations is difficult where the lines between categories and classifications of services and products are blurred.

#### Transnational Orientation

Al is inherently multifaceted, with applications and implications that extend beyond national borders. However, the absence of universally accepted global regulatory standards presents a formidable challenge. Coordinating with regulators across borders is essential to establish a cohesive framework that ensures responsible development and deployment of these technologies on an international scale. This requires collaborative efforts among nations and organizations to address issues of ethics, data privacy, and security while fostering innovation in a globally interconnected digital landscape.

#### Accountability

The rapid evolution and interconnectivity of modern business models pose a formidable challenge in attributing responsibility for potential harm. Determining liability in this dynamic landscape, where identifying the causal factors and accountable parties can be complicated and elusive. For example, if a self-driving car crashes and kills someone, it is challenging to determine the stakeholder who is liable. Is it the system's programmers, the driver, the car's manufacturer, or the manufacturer of the vehicle's onboard sensory equipment? The concept of accountability further stands challenged by the concept of reinforcement learning, a training method that allows AI to make decisions based on past experiences.

#### Personally Identifiable Sensitive Data Insecure

Al has changed the way personal information is processed and used to influence human behaviour. For an Al system to attain a high degree of reliability, there has to be extensive training on diverse datasets. However, gives rise to concerns regarding the potential for data breaches and unauthorized access to personal information. For e.g. the French data protection authority fined Clearview Al for violating EUGDPR by collecting and processing data of individuals residing in France without a legal basis for facial recognition<sup>4</sup>.

#### Power Imbalance and Information Asymmetry

The use of AI algorithms gives private companies an opportunity to gather detailed insight into one's personal circumstances and behavior patterns, offering a window into their lives. Companies can tailor their advertising, prices and contract terms to customer profileand thereby exploit the consumer. Certain markets, such as credit or insurance, operate on cost structures based on risk profiles correlated with features distinctive to individual consumers, suggesting that it may be reasonable to offer different prices (e.g., interest rates) to different consumers. It is challenging for regulators to map and mitigate discrimination in such cases.

#### **Understanding Black Box**

In AI systems, input to the model (called features) is provided along with the 'correct' output through annotated labels during training. The AI system then identifies the relationship between input features and labels. Understanding this relationship becomes harder as the models become increasingly complex. This manifests itself as the inability to fully understand an AI's decision-making process and the inability to predict decisions or outputs–also known as the "black box problem"<sup>5</sup>.

#### Bias

Al solutions have the potential to be 'biased' against specific sections of society. This can lead to inconsistent output across a similarly placed diverse demography. Real life manifestations of such bias tie into historically discriminatory behaviour, where members of a certain caste, class, sex or sexual orientation, among others, are denied opportunities on the basis of an identifying characteristic even though they are completely similar in all ways relevant to the decision being made<sup>6</sup>.



Hence, the primary goal of AI should be to foster the development of new and emerging technologies, concurrently with the mitigation of potential harms. Achieving this balance needs the implementation of innovative regulatory approaches, such as sandboxing. Sandboxing involves creating controlled environments where AI systems can be tested and refined, allowing regulators to closely monitor and understand their functions and risks. By embracing such methods, we can encourage technological innovation while proactively identifying and addressing any adverse consequences. This will ensure responsible and safe AI deployment and strike a harmonious equilibrium between progress and protection in the AI landscape.

### **Regulatory Sandbox**

A regulatory sandbox is an example of a "soft law" mechanism in emerging technologies, introduced in highly regulated industries such as finance and energy. This is also related to specific spheres or regulations, such as AI or GDPR, with the goal of promoting responsible innovation/and or competition, addressing regulatory barriers to innovation and advancing regulatory learning<sup>7</sup>. In a regulatory sandbox, new products or services are tested in a controlled environment with certain regulatory relaxations if required for testing with real consumers.

Sandbox tests are expected to have a clear objective and a positive impact on consumers. They are typically conducted on a small scale, for a limited duration, with a limited number of consumers. This allows evidence collection on the benefits and risks of innovative products and services to help regulation adapt to changing requirements fostering innovation. The suitability of the regulatory sandbox depends on the regulatory objectives, the flexibility of the existing regulatory regime, the resources and capacity of the regulator, and the types of innovations emerging in the market. Under certain circumstances, they have the potential to speed up the regulatory adaptation towards an enabling framework in support of inclusive, innovative, new and emerging technologies.

Generally, a regulatory sandbox goes through the following stages:



The table below depicts some of the prominent benefits and limitations related to regulatory sandboxes:

Benefits	Limitations
Empirical evidence	Loss of flexibility
Supports innovation	Discretional judgements
Improved understanding	Regulatory arbitrage
Consumer protection	Regulatory arbitrage
	High operation costs

According to the World Bank, there are 73 sandboxes operating across 57 jurisdictions<sup>8</sup>. The concept of a sandbox was introduced in 2015 by the Financial Conduct Authority (FCA), United Kingdom (UK) as a mechanism to allow fintech businesses 'to test innovative propositions in the market, with real consumers.' Following in the footsteps of the UK, regulatory sandboxes have gained significant traction and have been introduced in several countries, including Canada, Norway, Germany, Korea, UK, Singapore, Australia, Malaysia, and the United Arab Emirates, among others. The international practices of regulatory sandboxes are covered in detail in **Annexure 1**. We are also seeing the emergence of regulatory sandboxes for AI with countries such as Spain, Canada and Norway taking the lead in designing these. These sandboxes are also covered under **Annexure-1**.

India has demonstrated a proactive approach to the adoption of regulatory sandboxes, primarily within the fintech sector. This is clear from the issuance of guidelines by regulatory bodies such as the RBI and SEBI. Interestingly, the concept of regulatory sandboxes is now transcending the fintech domain. This is indicated by its incorporation into the Draft Telecom Bill and the State of Telangana's recent announcement of a regulatory sandbox tailored for Web 3 technologies. In 2021, the National Urban Digital Mission under the Ministry of Housing and Urban Affairs also released a concept note for U-Box which builds upon and expands on the scope of the conventional regulatory sector. These initiatives are explained in detail in **Annexure 2.** While India has adopted a regulatory sandbox, there have been challenges in optimizing its potential.

Some of these which must be addressed for a regulatory sandbox for AI as well are highlighted below:

#### Fragmented Approach

The current regulatory landscape is hampered by a fragmented approach, where each regulatory authority operates its own sandbox within its specific sector. This limits the scope of innovation and collaboration, as it fails to recognize the interconnectivity and cross-sectoral nature of AI. Each sector operates within its own regulatory framework results in disjointed efforts and inconsistent approaches. To overcome this challenge, it is crucial to adopt a more cohesive and integrated approach that transcends sectoral boundaries.

#### Lack of Uniformity in Frameworks

The lack of uniformity in sandbox frameworks across regulators poses challenges for businesses operating in multiple sectors. Varying approaches to key sandbox features, such as eligibility criteria, consumer protection requirements and duration, create inconsistencies and ambiguity. This lack of uniformity creates uncertainty for businesses seeking to participate in sandboxes, hindering their ability to innovate and navigate the regulatory landscape effectively.

#### Scalability and Interoperability

8

Integration of successful sandbox-tested solutions into the broader market infrastructure may encounter challenges related to scalability and interoperability with existing financial systems. These issues must be addressed to ensure that innovations developed within the sandbox can seamlessly integrate and operate within the existing regulatory framework and infrastructure.

# **Structure of AI Sandbox for India**

Based on the this analysis, we would like to recommend the following aspects which may be considered while defining the guidelines for regulatory sandboxes:

### **Regulatory Sandbox: Structure**

#### **Empirical Analysis**

The successful implementation of regulatory sandboxes in India faces a plethora of complex challenges. These encompass various facets, including the considerable financial resources required for setup and monitoring, the imperative to ensure that regulatory sandboxes yield the anticipated outcomes and benefits, the need to integrate them effectively within the broader regulatory ecosystem, and the critical task of balancing innovation with robust consumer protection measures. Given these challenges, it is imperative to conduct an empirical study of existing regulatory sandboxes in India. This can provide invaluable insights into their effectiveness and the nuances of the hurdles encountered during their implementation.

#### Incorporation of a Sandbox clause for AI

New and emerging technologies such as AI which s which do not fit into any of the existing laws, regulations and sandboxes should be covered under the regulatory sandbox under the Digital India Bill. It must also be kept in mind that the success of a regulatory sandbox for AI hinges on a robust commercial infrastructure that can support and fund innovative AI projects. Additionally, eliminating information asymmetry is vital, ensuring that all participants have equitable access to credible and diverse datasets. This creates a level playing field, enabling a more comprehensive exploration of AI's potential while mitigating disparities in resource availability, thereby enhancing the sandbox's efficacy in nurturing AI innovation.



#### **Empowered Committee**

An empowered committee may be set up under the Digital India Bill wherein it is granted enough flexibility to define sandboxes suitable for the needs of specific AI cohorts.

#### Structure of the Empowered Committee

- Under the Digital India Bill the Empowered Committee may be constituted by the Central Government.
- The Committee may consist of a chairperson and a number of other official and non-official members with special knowledge of law, technology, defining and operating sandboxes or any other expertise that the Central Government may prescribe through rules. The Committee can consist of ministries such as the Ministry of Electronics & Information Technology, Ministry of Law & Justice, Ministry of External Affairs, nodal ministry/regulator for the cohort, academia and industry.
- The sum total of Committee members, including the chairperson, should be an odd number.
- The Committee should, as far as possible, function as a digital office and employ such techno-legal measures as may be prescribed.
- The applicants along with the Committee should develop evaluation standards for emerging safety and security issues and otherwise contribute to the development of ecosystem functions to enhance the safety, security, and transparency of innovative products being tested.
- While defining the regulatory sandbox the Committee should be allowed to co-opt experts in that field and representatives of relevant ministries of the Central Government and sectoral regulators. This will ensure fair evaluation of applications and the developing of appropriate frameworks for cohorts of AI systems with adequate guardrails.
- The applicants along with Committee members and AI experts co-opted should ensure the implementation of robust reliability and safety practices for its high-risk models and applications ensuring a layered safety-by-design approach.

#### Who should be considered for the Empowered Committee

- Start-ups, innovators and corporates should be allowed to participate in the sandbox.
- Foreign entities seeking entry to India should also be allowed to participate. Reference in this case may be drawn from SEBI's Interoperable Regulatory Sandbox explained in detail in the section above.
- Applicants should demonstrate in the application that they possess the required financial and technological resources to take part in the sandboxing process.
- The product, service, concept should be innovative and add value.
- The need for testing in a live environment should be clearly established and existing challenges clearly established.
- Applicants should have appropriate risk mitigation strategies and ensure transparency about the nature and scope of testing. They should also demonstrate the consumer protection measures undertaken.

#### Sandbox Application, Testing and Exit

- It must be noted sandboxing is best aligned to the testing of applications and finished services. Typically, sandboxing is best aligned to AI application testing.
- Safety, security, and privacy should be key considerations in regulatory sandboxes as well. Security aspects such as red teaming must be considered for AI applications, even during regulatory sandbox.
- Application stage: The application stage should be clearly defined by the Committee which should not exceed 30 days. Where the application is rejected, clear reasons should also be provided.
- The scope of sandbox testing including what regulatory requirements are being complied with and what exemptions from the existing regulatory regime pertaining to the product/service/application are sought under Sandbox testing should be defined in consultation with the applicant e.g. Sandbox to test the safety of a specific set of high-risk scenarios or defined use cases.
- To ensure the scalability and viability of the sandbox due recognition should be given to key elements of the AI technology stack such as model alignment, meta-prompt, application etc. Without due recognition of these elements, it would result in sandbox testing end-to-end safety of AI systems which may result in extremely high requirements to deal with high-risk AI systems or extremely low criteria to ensure that any application of AI can be included.
- Whether the Committee is willing to allow regulatory exemptions should be communicated at the earliest and a maximum time limit may be prescribed within this has to be communicated to the applicant.
- If the applicant is able and willing to meet the proposed regulatory requirements and conditions, he or she should be granted permission to develop and test the proposed innovation in the sandbox.
- The applicant should get positive consent from the users/consumers for participating in the testing.
- In case there are any material changes to the innovative solution during the testing phase, the same should be communicated to the Committee along with its reason. Post this, the Committee's decision should be final if it says it would like to continue the solution in the sandbox testing.
- The duration of the sandbox testing should also be clearly defined by the Committee in consultation with the cohort, with strict exceptions for the extension of time built in in genuine cases.
- The sandbox regulations should include a clear exit and deployment strategy that outlines the process for exiting the testing phase and launching the product/service/technology in the wider market. The impact of the exit on on-boarded customers should be clearly defined in the application and also conveyed to such customers.



### **Designing Regulatory Sandboxes: General aspects**

#### Clear Definition of the Scope of Regulatory Sandbox

- New & emerging tech such as AI often poses new challenges to existing regulations and regulators. Therefore, a clear definition of the scope of the regulatory sandbox and relaxations should be considered to address these challenges for protecting consumers and fostering innovation.
- Aspects like immunity, liability, and what happens to the data collected during the regulatory sandbox need to be clearly defined. For example, in the regulatory sandbox by RBI, the central -bank is exempt from any kind of liability but the applicants are not. This might go against the nature of the regulatory sandbox. A practice that can be considered is to have a tripartite agreement between the Committee, cohort and the consumers defining liability in clear terms, keeping in mind what is permissible under the law.

#### **Streamlined Application Process**

Many early sandbox initiatives adopted elaborate application processes. As a result, there are lengthy written applications which provide no actual insight into the nature of the innovation to be tested. A sharpened application process which significantly reduces the time-consuming process and onboards companies faster would go a long way towards streamlining the process.

#### Defining Initial Regulation for the Sandbox

The regulators work with the cohort to define the initial regulations. The focus in the initial stage should be on broad-based regulations to promote innovation, protect consumers and create a grievance redressal mechanism. This set of recommendations should be flexible during the period of the sandbox cohort. The regulators should have the power to co-opt technical experts and members from relevant ministries to ensure the effective design of the initial regulation.

#### Determine a Reasonable Timeframe for Sandbox Testing

Allow participants sufficient time to validate their products or services while avoiding unnecessary delays. Consider phased testing periods to assess different aspects of the innovation, progressively expanding the scope and scale of the experiments.

#### Corporates

Organizations that are no longer start-ups but have sufficient experience in the field should also be allowed to apply to be part of the sandbox provided they prove their technical proficiency in the field as per the guidelines laid out with each cohort's application.

#### **Foreign Entities**

Foreign entities seeking entry to India, should also be allowed to participate in the sandbox. Reference in this case may be drawn from SEBI's Interoperable Regulatory Sandbox explained in detail above.

### **Post-sandbox activities**

#### **Disclosures**

- To ensure transparency the Committee should make requisite disclosures. Disclosures for a regulatory sandbox in AI should relate to aspects relating to where the high impact models are being deployed and developed, and the customers accessing such AI models. The high-impact models should also be required to label their content stating that it has been produced by AI.
- It is essential to facilitate community access to regulatory sandboxes, particularly for low-risk AI models.
   To enhance transparency, the sandbox's requirements can be made publicly available on platforms like
   Mygov. While ensuring transparency, it is crucial to respect Intellectual Property Rights and exempt
   proprietary materials from publication when disclosing the sandbox's results.

#### **Building Cross-Sector Regulatory Communication Channels**

- Cross-border collaboration must also be ensured. Models that are already tested in other countries should be able to make their way to India without the need for a regulatory sandbox. Reference may be drawn from similar arrangements such as the Common Criteria Recognition Experiment for testing For example the NIST AI Risk Management Framework (AI RMF) is intended for voluntary use and to improve the ability to incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems. If AI products, services and system follows these guidelines these products etc. should be able to make their way to India.
- In cases where post the regulatory sandbox is over, if the Committee feels that there are certain overlaps with any sectoral regulators/ sandboxes, it should offer these learnings to such sectoral regulators/ sandboxes instead of the cohort which needs to apply separately to such sandboxes.

#### **Cross-border Collaboration**

- Cross-border collaboration must also be ensured. Models that are already tested in other countries should be able to make their way to India without the need for a regulatory sandbox. Reference may be drawn from similar arrangements such as the Common Criteria Recognition Experiment for testing.
- One need not always re-invent the wheel. We should analyse the lessons learnt from already existing regulatory sandboxes on AI and differentiate which aspects we cannot implement owing to our unique requirements and mission objective.

#### Impact of the Sandbox

- The learnings of the sandbox in appropriate cases should translate into changes at the law and policy levels. Beneficial innovation reference in this regard can be drawn from the EU model of regulatory sandbox for the AI Act.
- Where, in the opinion of the Committee, there is a need to amend any applicable law or enact a new law (including Acts, rules, regulations and directions), then the empowered committee should recommend this to the relevant nodal ministry/regulator and the law ministry.

### Recommendation

Based on the comprehensive examination conducted, we recommend that the Ministry of Electronics & Information Technology undertakes the strategic development of a regulatory sandbox tailored for the field of AI. To ensure that this initiative is well-rounded and effective, it is crucial to initiate and sustain a process of extensive public consultation. By proactively engaging stakeholders from diverse backgrounds and expertise, the sandbox can be designed to address the varied challenges and opportunities associated with AI innovation. Public consultation will serve to promote transparency, inclusivity, and accountability in the sandbox's design and implementation.

Beyond the establishment of a regulatory sandbox, there is an urgent need for the government to prioritize the creation of robust governance frameworks that foster responsible AI practices. This can be achieved through a multi-pronged approach. Industry stakeholders should be encouraged to voluntarily adopt codes of conduct and engage in self-regulation, aligning their operations with responsible AI principles and established guidelines.

The introduction of governance sandboxes can help systematically achieve a conducive governance ecosystem. By seamlessly integrating the elements mentioned below, the government can establish an ecosystem that not only encourages AI innovation but also ensures that AI technologies are harnessed in a responsible, ethical, and beneficial manner.

**Step 1:** Serving as a dynamic testing ground. This would enable the development of standards similar to the NIST AI Risk Framework and ISO SC42 AI Management Standards ensuring governance of AI as technology.

**Step 2:** Enabling policymakers to assess the practical implications of proposed regulations and guidelines in real-world AI applications.

**Step 3:** Leveraging existing regulatory frameworks and legislation to provide a foundation for responsible AI governance.

This holistic approach safeguards the interests of both industry and society, contributing to the responsible advancement of AI technology while mitigating potential risks and ethical concerns associated with its proliferation.



### Annexure-1

# Global Scenario of Regulatory Sandboxes

Торіс	Description	
	Kingdom of Saudi Arabia <sup>9</sup>	
Nodal Authority	Communication, Space & Technology Commission	
Sector	Emerging Tech	
Targeted Technologies	<ul> <li>Internet of Things (IoT)</li> <li>Blockchain</li> <li>Augmented Reality/Virtual Reality/Extended Reality (AR/VR/XR)</li> <li>Digital Twin</li> <li>3D/4D printing</li> <li>Cloud computing</li> </ul>	
Prominent Requirement	<ul> <li>Readiness of innovative business model, solution, and service</li> <li>Rely (business model, solution, and service) on emerging technologies.</li> <li>Demonstrate clear benefits to end customers.</li> <li>Provide a clear plan for participation and testing of the business model, solution, and service.</li> <li>Plan to launch commercially or scale the business in Saudi Arabia</li> </ul>	
Relaxations	• The nodal body may consider whether a particular regulatory requirement can be temporarily amended during the test period if the regulation or requirement was enacted by CITC itself. This will not be considered where the testing has a medium to high risk of causing harm to consumers.	
	UK <sup>10</sup>	
Sector	• Financial	
Nodal Body	Financial Conduct Authority	
Relaxations	<ul> <li>Help in identifying existing relevant rules and guidance applicable to the proposed business model.</li> <li>An informal steer to help firms understand the potential regulatory implications of their innovative product or business model. Informal steers are provided on specific regulatory issues and the implications of an innovative product or business model that is at an early stage of development.</li> <li>Individual guidance to explain how the nodal body will interpret the requirements in the context of innovative product-specific testing.</li> <li>Waive or modify an overly difficult rule for the test. No waiver for national or international law.</li> <li>No enforcement action letters where FCA can't issue individual guidance or waivers, but believe it's justified considering the circumstances of the sandbox test. The letter would only apply for the duration of the sandbox test and only FCA's disciplinary action. It wouldn't limit any liabilities to consumers.</li> </ul>	
Other notable initiatives	<ul> <li>Innovation Pathways: For firms that are not ready to test but need help understanding the FCA regulatory regime.</li> <li>Digital Sandbox: An online platform aimed at early-stage development propositions, where firms can access data sets to test and build prototype solutions.</li> </ul>	

9. https://www.cst.gov.sa/en/services/Documents/CITC\_Emerging\_Technology\_Regulatory\_Sandbox\_Guideline.pdf

10. https://www.fca.org.uk/firms/innovation/regulatory-sandbox

Note: Similar structure is also available for emerging technologies, biometrics, and exceptional innovations which is under the Information Commissioner's Office. <sup><math>n</math></sup>	
	Kenya <sup>12</sup>
Sector	Emerging Technologies
Authority	Communications Authority     of Kenya
Relaxations	<ul> <li>Safeguards Plans to determine the specific regulatory requirements it has prepared to temporarily modify during a regulatory sandbox test on a case-by-case basis.</li> </ul>
	Japan <sup>13</sup>
Sector	· All
Authority	Japan Economic Revitalization Bureau of the Cabinet Secretariat
UN <sup>14</sup>	
Description	<ul> <li>The UN Development Account Project "Frontier Technology Policy Experimentation and Regulatory Sandboxes in Asia and the Pacific" has been conceived and approved, with the objective of enhancing the institutional capacity of selected countries in special situations to understand and develop digital technologies' policy experimentation and regulatory sandboxes. The Project is jointly implemented by UN DESA and UN ESCAP. Since the inception of the Project, the implementation has gained traction in all three target countriesBangladesh, Kazakhstan and Maldives, with political leadership and substantive commitment from all three countries.</li> </ul>
	France Expérimentation <sup>15</sup>
Authority	French Ministry of Economy and Finance
Description	<ul> <li>France Experimentation – Administration is a device for the decentralised services of the State. It aims to remove unresolved administrative and legal bottlenecks at the local level, to accelerate projects with a significant economic impact. All innovative products and services are eligible for this sandbox initiative, and not just those based on new and emerging technologies. Projects span a wide range of sectors, including real estate, biotechnology, micro-credit, health, energy performance and waste treatment.</li> </ul>
	Germany <sup>16</sup>
Authority	German Federal Ministry for Economic Affairs and Energy (BMWi)
Description	<ul> <li>The BMWi published a Regulatory Sandbox Strategy in December 2018. The Regulatory Sandboxes Strategy seeks to systemically establish regulatory sandboxes in Germany. It consists of three pillars: 1) fostering greater use and development of experimentation clauses, 2) providing information and networking to facilitate the creation of regulatory sandboxes (e.g. by a regulatory sandbox handbook and a regulatory sandbox network), and 3) launching and supporting regulatory sandboxes through competitions or support for specific projects. The strategy does not focus on one specific field of innovation, but rather on regulatory sandboxes as a cross-cutting instrument useful for different fields of innovation</li> </ul>

https://ico.org.uk/for-organisations/advice-and-services/regulatory-sandbox/our-key-areas-of-focus-for-the-regulatory-sandbox/ https://www.ca.go.ke/wp-content/uploads/2023/01/Framework-for-Emerging-Technologies-Regulatory-Sandbox-January-2023.docx.pdf 12.

https://www.japan.go.jp/abenomics/regulatory/sandbox/index.html 13.

<sup>14.</sup> https://www.un.org/development/desa/dpad/wp-content/uploads/sites/45/publication/PB\_123.pdf

<sup>15.</sup> https://www.modernisation.gouv.fr/nos-actions/france-experimentation

<sup>16.</sup>  $https://www.bmwk.de/Redaktion/EN/Publikationen/Digitale-Welt/handbook-regulatory-sandboxes.pdf?\_blob=publicationFile\&v=2$ 

Mauritius <sup>17</sup>	
Authority	Mauritius Economic Development Board (MEDB)
Description	<ul> <li>The Regulatory Sandbox License operated by the MEDB was officially launched in 2016 and is intended to operate in areas in which there are no existing laws or regulations. While many of the projects involve financial products and services, it is available for innovations in general. One of the criteria for eligibility when applying to this sandbox programme is the need to contribute to the development of local skills and knowhow in Mauritius. In particular, projects that foster the Mauritian economy, including greater accessibility, efficiency, security, reliability or effectiveness in the provision of services and products in diverse sectors, are prioritized.</li> </ul>
	Canada <sup>18</sup>
Description	<ul> <li>The Global Financial Innovation Network (GFIN) has been pushing for the creation of a "global sandbox" using an international legal compatibility initiative between its members to implement simultaneous testing processes in different institutions. Bedrock AI was one of two companies to enter the GFIN cross-testing initiative. The Alberta Securities Commission, Quebec's Autorité des Marches financiers, the British Columbia Securities Commission, and the Ontario Securities Commission approved Bedrock AI to test its machine-learning solutions to identify (WHAT IS FLAGS?) flags in Canadian corporate disclosure agreements.</li> </ul>
	EU <sup>19</sup>
	<ul> <li>Spain launched an AI regulatory sandbox in 2022 as the first pilot program to test the future EU AI Act. Spain's initiative is undertaken with the EC and seeks to onboard other EU members. Uniquely, the Spanish AI sandbox was established to test a regulation that has neither been finalised nor entered into force (the EU AI Act is expected to enter into force in 2025). The goal is to test the proposed regulatory framework with real AI applications to assess how the regulation and application-development respond and to suggest modifications or explanatory guidelines. Both Spain and the EC put forward that the pilot AI sandbox will test other regulatory experimentation mechanisms such as AI standards, and Testing and Experimentation Facilities (TEFs). TEFs provide a framework, tools and infrastructure to test innovative AI products, including how they comply with regulatory requirements. Regulatory sandboxes can also provide valuable insights into standardisation processes. Practical implementation of the proposed EU AI Act's requirements for high-risk AI systems will provide use cases examining how those requirements could be developed. Standards and TEFs could play a crucial role in the testing phase of regulatory sandboxes. On the one hand, standards. On the other hand, TEFs can provide the technical backbone for AI sandboxes in certain instances, and the technical infrastructure necessary to test certain AI applications. According to Spain, future regulatory trends will be to create international clusters of AI sandboxes enabling cross-testing.</li> <li>Until then, a sequential approach could be taken that includes:</li> <li>A national phase, during which AI regulatory sandboxes are used at national level to enable regulators to gather data, improve practices, optimise internal testing processes, and issue public guidelines to improve firms' legal certainty.</li> <li>An international phase, with mechanisms to encourage participation by public (e.g. competent national authorities) and p</li></ul>

<sup>17.</sup> 

The role of sandboxes in promoting flexibility and innovation in the digital age (oecd.org) https://www.oecd-ilibrary.org/docserver/8f80a0e6-en.pdf?expires=1690537598&id=id&accname=guest&checksum=EB62628EE5E2AEEC3BC02C7C3BFFA826 https://www.oecd-ilibrary.org/docserver/8f80a0e6-en.pdf?expires=1690537598&id=id&accname=guest&checksum=EB62628EE5E2AEEC3BC02C7C3BFFA826 18.

Norway regulatory sandbox for Al <sup>20</sup>	
Authority	Norwegian Data Protection Authority's
Objective	• The overall objective is to stimulate the innovation of ethical and responsible AI.
Methodology	<ul> <li>In the sandbox, businesses will be given the opportunity to develop innovative services within given frameworks and under guidance from the Norwegian Data Protection Authority. Sandkassen shall not grant dispensation from the Personal Data Act, but shall be able to grant dispensation from enforcement measures in the development phase of the project.</li> </ul>
Singapore <sup>21</sup>	
Authority	Monetary Authority of Singapore (MAS)
Details	<ul> <li>The MAS facilitates live testing of AI applications.</li> <li>Based on the learnings of the regulatory sandbox, MAS released a set of principles to promote Fairness, Ethics, Accountability, and Transparency (FEAT) in the use of AI and data analytics in the financial sector.</li> <li>The FEAT principles were also released as part of Singapore's National AI Strategy to build a progressive and trusted environment for AI adoption in this sector.</li> </ul>

https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/regulatorisk-sandkasse-for-utvikling-av-ansvarlig-kunstig-intelligens/
 https://www.oecd-ilibrary.org/docserver/8f80a0e6-en.pdf?expires=1695116827&id=id&accname=guest&checksum=5AB0ADBFC1881171509BF43E50E8F7ACer/ 8f80a0e6-en.pdf?expires=1695116827&id=id&accname=guest&checksum=5AB0ADBFC1881171509BF43E50E8F7AC

#### Annexure-2

## Regulatory Sandboxes in IndiaSandboxes

Торіс	Description
	RBI <sup>22</sup>
Sector	• Fintech
Focus Area	<ul> <li>There is an absence of governing regulations.</li> <li>There is a need to temporarily ease regulations for enabling the proposed innovation.</li> <li>The proposed innovation shows promise of easing/effecting delivery of financial services in a significant way.</li> </ul>
Applicable: Products/Services/ Technology	<ul> <li>Retail payments</li> <li>Money transfer services</li> <li>Marketplace lending</li> <li>Digital KYC and digital identification services</li> <li>Financial advisory and wealth management services</li> <li>Smart contracts</li> <li>Financial inclusion products</li> <li>Cyber security products</li> <li>RegTech and SupTech</li> <li>Mobile technology applications (payments and digital identity)</li> <li>Data analytics</li> <li>Application Program Interface (APIs) services</li> <li>Applications under block chain technologies</li> <li>Al and Machine Learning applications</li> </ul>
Not Applicable: Products/Services/ Technology	<ul> <li>Readiness of innovative business model, solution, and service</li> <li>Rely (business model, solution, and service) on emerging technologies.</li> <li>Demonstrate clear benefits to end customers.</li> <li>Provide a clear plan for participation and testing of the business model, solution, and service.</li> <li>Plan to launch commercially or scale the business in Saudi Arabia</li> </ul>
Relaxations available for	• The nodal body may consider whether a particular regulatory requirement can be temporarily amended during the test period if the regulation or requirement was enacted by CITC itself. This will not be considered where the testing has a medium to high risk of causing harm to consumers.
No relaxations avail- able for	<ul> <li>Customer privacy and data protection</li> <li>Secure storage of and access to payment data of stakeholders</li> <li>Local data storage</li> <li>Security of transactions</li> <li>KYC/AML/CFT requirements</li> <li>Statutory restrictions</li> </ul>

SEBI <sup>23</sup>	
Securities & Commodities	
• All entities registered with SEBI under section 12 of the SEBI Act 1992.	
<ul> <li>Stage–I: SEBI will approve the limited set of users as proposed by the applicant for testing in Stage-I. During the Stage-I testing, applicant shall use limited and identified set of users with maximum cap on users based on the requirement of the applicant duly approved by SEBI on a case-to-case basis. These users will be required to provide positive consent, including their understanding of the risks of using the solution.</li> <li>Stage–II: During the Stage-II testing, applicant shall test with a larger set of identified users with maximum cap on users based on the requirement of the applicant duly approved by SEBI on a case-by-case basis. These users will be required to provide positive consent including understanding of the risks of using the solution.</li> </ul>	
<ul> <li>Genuine need to test.</li> <li>Genuine relaxation</li> <li>The solution should be either a new solution or improvement in the existing processes.</li> <li>Identified benefits to the users and/or the securities/commodities markets.</li> <li>Intent and feasibility to deploy the proposed innovative solution post testing.</li> </ul>	
<ul> <li>Applicant has achieved adequate progress in Stage –I testing.</li> <li>Review of the risks observed during Stage –I testing.</li> <li>Review of the steps taken to mitigate risks.</li> <li>Appropriate safeguards to manage risks and contain the consequences of failure.</li> <li>User feedback during Stage-I testing.</li> <li>Intent and feasibility to deploy the proposed innovative solution post testing.</li> </ul>	
<ul> <li>From the extant investor protection framework,</li> <li>Know-Your-Customer (KYC)</li> <li>and Anti-Money Laundering (AML) rules.</li> </ul>	
Draft Telecom Bill <sup>24</sup>	
• Telecom	
<ul> <li>The bill recognizes the concept of regulatory sandbox and provides for a set of special terms and conditions to promote innovation and R&amp;D through rules.</li> <li>The objective is to facilitate the development of telecom technologies and generate new employment.</li> <li>The focus is on empowering the startup ecosystem</li> </ul>	
Emerging Technologies IT&C Department, Karnataka <sup>25</sup>	
• Web 3.0	
<ul> <li>Start-ups</li> <li>Innovators</li> <li>Corporates</li> </ul>	
<ul> <li>The sandbox will operate in a continuous format.</li> <li>The participants can exit the sandbox as and when they are through with their testing process. However, the testing period for a participant may not exceed 6 months.</li> <li>The application will be reviewed by the governing council at each meeting after which the approved participants will be onboarded.</li> <li>Initially, the size of active participants in the sandbox is expected to be kept at about 10-15. This may be increased later.</li> <li>The observations on regulatory policies will be passed on to the regulatory bodies and wherever necessary state-level policies will be drafted to implement findings from the sandbox.</li> </ul>	

https://www.sebi.gov.in/legal/circulars/jun-2021/revised-framework-for-regulatory-sandbox\_50521.html https://dot.gov.in/sites/default/files/Draft%20Indian%20Telecommunication%20Bill%2C%202022.pdf 23.

24.

25. https://web3sandbox.telangana.gov.in/

National Urban Digital Mission <sup>26</sup>	
Sector	Urban Development Sector
Description	<ul> <li>A multi-functional sandboxU-Boxs proposed to be established for serving the innovation needs of the urban development sector in an integrated manner.</li> <li>U-Box builds on and expands the scope of the conventional 'regulatory sandbox', by adding to it the dimensions of digital technologies, emerging technologies, business models, proof-of-value, and regulated access to production data.</li> </ul>
Functions	<ul> <li>Testing of digital technologies</li> <li>Testing of emerging technologies</li> <li>Conformance to regulations</li> <li>Proof-of-value</li> <li>Business viability</li> </ul>
Pension Fund Regulatory and Development Authority <sup>27</sup>	
Sector	• Fintech
Ambit	<ul> <li>Inter-operable regulatory sandbox with a mechanism to facilitate testing of innovative hybrid financial products/services falling within the regulatory ambit of more than one financial sector regulator.</li> </ul>
Eligibility	• Type of enhancement to existing products like loans, deposits, capital market instruments, insurance, G-sec instruments and pension products.
	SEBI's Interoperable Regulatory Sandbox <sup>28</sup>
Sector	• Fintech
Participating or- ganization	<ul> <li>Inter-Regulatory Technical Group on FinTech- The Group is chaired by Chief General Manager of the FinTech Department, RBI with representation from other financial sector regulators, viz., SEBI, IRDAI, IFSCA and PFRDA and one representative each from DEA and MeITY.</li> </ul>
Governance	<ul> <li>The RS framework of the regulator under whose remit the 'dominant feature' of the product falls, shall govern it as 'Principal Regulator (PR)'. The regulator/s under whose remit the other features apart from the dominant feature of the product fall shall be the 'Associate Regulator (AR)'.</li> <li>Detailed scrutiny of the application shall be done by the PR based on its own framework. The PR shall coordinate with AR(s), regarding the features of the product, which falls under its remit.</li> <li>Applications from Indian fintechs having global ambition and foreign fintechs seeking entry to India, shall be referred to IFSCA, for taking forward the proposals, as IFSCA will be the PR for all such applications.</li> <li>The test design shall be finalised by the PR in consultation with the AR.</li> </ul>
Exposure draft on IRDAI (Regulatory Sandbox) Regulations, 2019 <sup>29</sup>	
Sector	• Insuretech
Ambit	<ul> <li>Insurance solicitation or distribution</li> <li>Insurance products</li> <li>Underwriting</li> <li>Policy and claims servicing</li> <li>Any other category recognised by the Authority.</li> </ul>

- $\label{eq:27} https://www.npscra.nsdl.co.in/download/Responsible \% 20 Innovation \% 20 through \% 20 Regulatory \% 20 Sandbox (RS).pdf$
- 28. https://www.sebi.gov.in/sebi\_data/commondocs/oct-2022/SoP%20for%20Interoperable%20Regulatory%20Sandbox\_Final\_p.pdf

29. https://irdai.gov.in/document-detail?documentId=391491

Maharashtra <sup>30</sup>	
Sector	• Fintech
Focus Area	<ul> <li>API Sandbox: API Sandbox provides a platform for financial institutions, fintech and startups to exchange data through application programming interfaces (APIs). API Sandbox promotes open banking platform via APIs for faster innovation and integration of new and legacy IT systems.</li> </ul>
Ambit	<ul> <li>Insurance tech</li> <li>Investment tech</li> <li>ROBO advisory</li> <li>Forex</li> <li>Security</li> <li>Blockchain applications</li> <li>Machine Learning</li> <li>Education</li> </ul>

25

# **ABOUT AUTHORS**

Tanvi Sharma Associate tsharma@chase-india.com

Srishti Saxena Account Director ssaxena@chase-india.com Dr. Dhawal Gupta Group Business Director dhawalg@chase-india.com

Kaushal Mahan Vice President kaushal@chase-india.com

# **ABOUT CHASE INDIA**

Founded in 2011, Chase India is a leading public policy research and advisory firm with growing practices in Technology & Fintech, Transport & Infrastructure, Healthcare & Life Sciences, Development and Sustainability. We provide consultancy services to organizations for mitigating business risks through insight-based policy advocacy. Over the years, Chase India has collaboratively worked with multiple stakeholders such as government, parliamentarians, civil society organizations, academia and corporates on several policy issues of critical importance. Chase India is committed to using its knowledge, high-ethical standards and result-oriented approach to drive positive action for our partners. Chase India has pan India presence with offices in New Delhi, Mumbai, Pune, Hyderabad, Chennai and Bengaluru and is a part of the WE Communications Group worldwide. For more information, please visit <u>www.chase-india.com.</u>



#### DISCLAIMER

Neither Chase Avian Communications Private Limited (referred to as "Chase India"), nor Consumer VOICE, nor agency thereof, nor any of their employees, nor any of their contractors, subcontractors or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or any third party's use or the results of such use of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific organization, commercial product, process or service by trade name, trademark, manufacturer or otherwise does not necessarily constitute or imply its endorsement, recommendation or favouring by the Organizer or any agency thereof or its contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of Chase India or Consumer VOICE, or any agency thereof.

For more information, please visit www.chase-india.com

