DATASPHERE INITIATIVE

AI sandboxes and the private sector

Emerging models and opportunities

About the Datasphere Initiative

The Datasphere Initiative is a think and do tank that catalyzes meaningful dialogues and co-creates actionable and innovative approaches to respond to data challenges and harness opportunities across borders. Our mission is to equip organizations to responsibly unlock the value of data for all. For more information, visit www.thedatasphere.org or contact info@thedatasphere.org.

About this report

This report is part of an informational series on AI Sandboxes from the Datasphere Initiative.

The report was first shared with experts in 2025 within the Global Sandboxes Forum Expert Group and discussed as a working paper presented at the Global Sandboxes Forum Insights Session Business and AI sandboxes in April 2026.

The report provides an overview of the opportunities and learnings when businesses engage in AI sandboxes and how operational and hybrid AI sandboxes support innovation and address AI safety and trust. The report shares insights for policymakers and regulators designing AI sandboxes to raise awareness of the types of barriers businesses face or incentives that can motivate their participation. It aims to contribute to building mutual understanding between public and private actors, so that sandboxes can achieve their real potential of enabling responsible AI innovation. Businesses can use the report to learn more about AI sandboxes and the implications of engagement. Public officials can use the report for guidance on setting up AI sandboxes that are attractive to business.

Table of contents

Acknowledgements

When preparing this report, the Datasphere Initiative team held consultations with various stakeholders in the form of in-person and online meetings. The report has however been drafted under the sole responsibility of the Datasphere Initiative and does not engage the actors listed. The Datasphere Initiative is thankful to all those who shared their expertise and experience which helped the production of the report.

Datasphere Initiative team: **Lorrayne Porciuncula**, Executive Director, **Sophie Tomlinson**, Deputy Executive Director, **Maria Marinho**, Director of Research, **Mariana Rozo-Paz**, Policy, Research and Project Management Lead, **Morine Amutorine**, Lead Africa Sandboxes Forum, **Risper Onyango**, Research Associate, **Thiago Guimaraes Moraes**, Senior Fellow, **Leticia Andrade,** Junior Research Analyst.

Contributors in their personal capacity during the GSF Insights session on April 16 2026 and peer review included: **Jennings Balavari,** Founder, Opsen AI, **Hannah Bowden,** UK AI Airlock Programme Delivery Lead, **Lucia Canga Roza,** Senior Managing Counsel (VP) Privacy, AI & Data Responsibility, Mastercard, **Mariana Luísa da Costa Lage**, **Albert Franca Josuá Costa, Marcus Vinicicus Rossi da Rocha, Diego André Sant´Ana**, ANDP, **Mia Hoffmann,** AI Quality Architect, Resaro AI, **Karan Jain,** Founder and CEO, NayaOne, **Sam Jungyun Choi,** Lawyer, Covington & Burling LLP, **Simon McDougall,** Chief Strategist, Privacy & AI, ZoomInfo, **Raíssa Moura,** Data Protection Officer, Nubank, **Henrik Netland Svensen,** Sandbox Coordinator, Datatilsynet, **Carolyn Nguyen**, Board Member, Datasphere Initiative **Wen Rui Tan,** Senior Manager (AI Governance), Singapore IMDA, **Timea Suto,** Global Digital Policy Lead, International Chamber of Commerce, **Fazliddin Tojiboev,** Digital Economy Research Center under the Ministry of Digital Technologies of Uzbekistan.

The report counted with editorial and design support from **Maíra Carvalho**, Director of Communications, and **Barbara Miranda**, Design Thinking Lead of the Datasphere Initiative.

Executive Summary

Businesses are navigating a dual imperative: intense commercial pressure to adopt artificial intelligence (AI) tools rapidly, and a deeply fragmented, uncertain regulatory landscape. Sandboxes have transitioned from niche fintech experiments into key tools for AI governance. Regardless of the maturity of AI development or the chosen regulatory regime, a range of governments and private institutions continue to set up these frameworks. Moving beyond the traditional public-sector lens, this report explores the concrete private-sector value derived from participation and outlines the distinct roles businesses of all sizes can take up.

Building on the sandbox definitions introduced by the Datasphere Initiative in the *Sandboxes for Data report* (2022),[1] and updated in the recent report *Sandboxes for Digital Public Infrastructure* (2026)[2] This report defines an **AI sandbox** as:

"a controlled learning environment in which AI systems, use cases, or related governance approaches are tested under defined conditions, timeframes, and safeguards, enabling iterative experimentation, evidence generation, and shared learning among multiple stakeholders to inform both innovation and governance."

By decoding current AI sandbox models and analyzing the concrete rationales, opportunities, and limitations for the private sector, this report seeks to bridge the gap between abstract policy design and real-world sandbox execution, providing businesses and policymakers with a more grounded understanding of how AI sandboxes can be used to test policy approaches and the business models designing or deploying AI in practice.

[1] In 2022 the Datasphere Initiative defined sandboxes as "safe spaces to test new technologies and practices against regulatory frameworks or experiment with innovative uses and means of governing data". Since then, the concept has evolved, which merited a new updated definition.

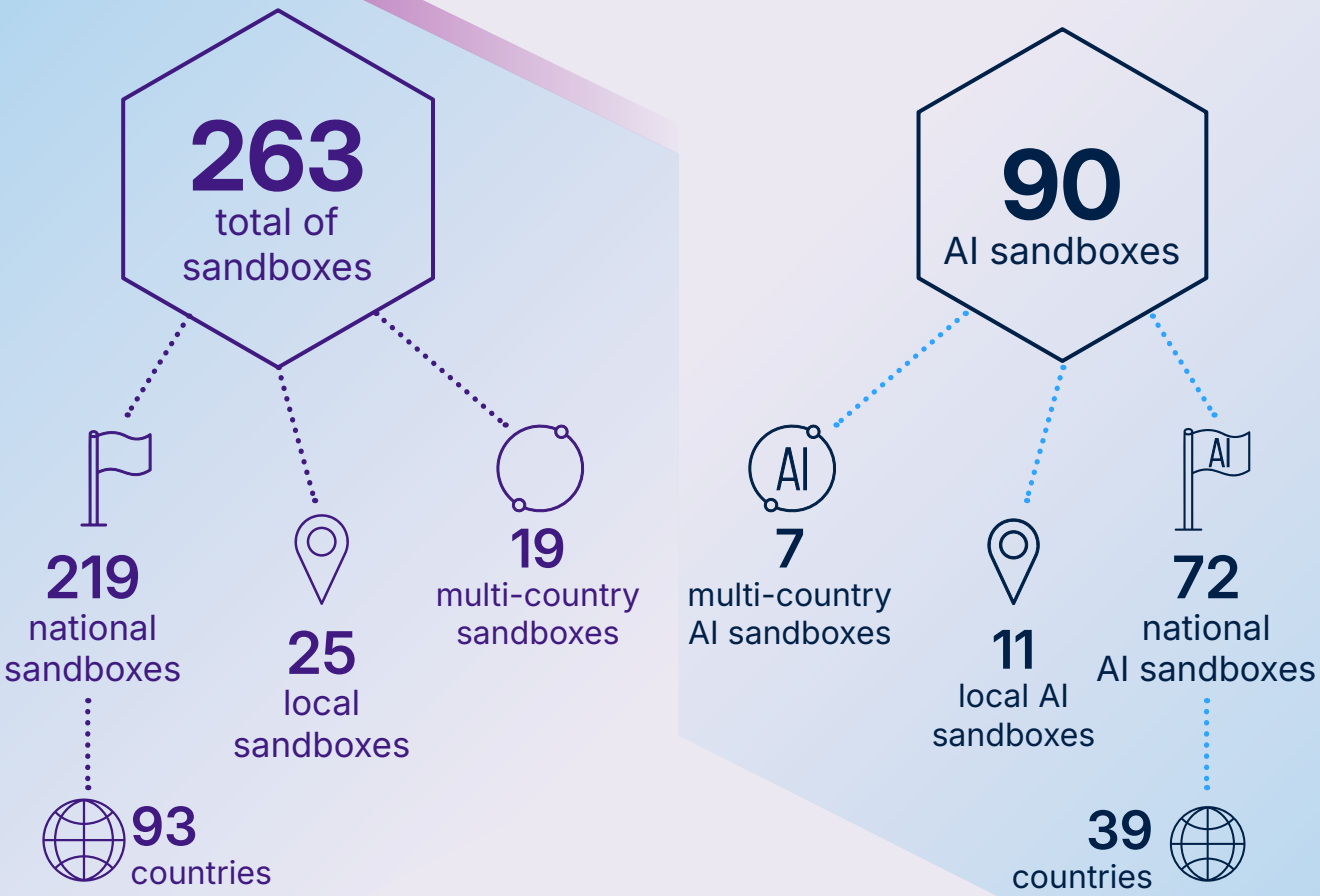
[2] Datasphere Initiative (2026), Sandboxes for DPI: Co-creating the blocks of digital trust, Datasphere Initiative.

The AI sandbox landscape: Core trends from our research

The analysis leverages an updated global tracking of **90 AI sandboxes across 39 countries**[3] updating the first global mapping produced by the Datasphere Initiative in 2025[4] and offering a global baseline of how AI sandboxes are evolving across continents and domains. Through meetings held in the context of the Global Sandboxes Forum and assessment of sandbox case studies and emerging best practices, the report outlines the roles companies can take up in AI sandbox models and the potential value these initiatives can bring.

AI Sandboxes at a glance

A global snapshot of AI sandbox ecosystems and their reach



AI sandboxes are expanding across countries and borders, driving innovation while supporting responsible governance.

[3] The Datasphere Initiative plans to launch an online platform with its global sandbox mapping by the end of 2026, and this report provides a sneak peak of its latest data on AI sandboxes

[4] Datasphere Initiative (2025), Sandboxes for AI: Tools for a new frontier, Datasphere Initiative.

Key takeaways

Several opportunities but also pressing challenges to private sector engagement in AI sandbox models are emerging. The key takeaways below provide high-level summaries of where the private sector can find value in AI sandbox models and where there remains persisting barriers or disincentives.

1 While AI sandboxes are on the rise, the **public sector needs more knowledge and capacity to effectively engage the private sector** as meaningful participants in regulatory and hybrid models.

2 A businesses' approach to AI sandboxes is dictated by its size, market position, and technical baseline. These capabilities shape how a firm balances operational risk against commercial upside, structuring their involvement into three core roles: **participants, technical providers, or sandbox hosts**.

3 The private sector isn't approaching AI sandboxes from a purely regulatory compliance perspective, but also as **experimentation spaces to test AI performance, business risks** and **organizational fit, develop proof of concepts, access data** and **run AI models in simulated or real-world environments** with **expert input**.

4 Several aspects of regulatory and hybrid AI sandboxes can deter private sector participation. Common concerns include **uncertainty around prospective impact, intellectual property, confidentiality, data access, security**, and **liability**. **Limited sandbox scopes, rigid oversight structures**, or **lengthy review processes as well as limited opportunities to test in "real world"** conditions can also deter private sector participation.

5 Persistent questions for the private sector are **what happens after a regulatory sandbox ends** and **how can sandbox learnings be leveraged across markets?** Solutions developed within sandboxes often struggle to transition into real-world deployment, particularly when moving across jurisdictions or regulatory regimes. This highlights a need for **more cross-regulatory** and **cross-border sandbox models**.

Recommendations for policymakers

The report identifies a series of recommendations for policymakers who are looking to attract private sector participants to their regulatory or hybrid AI sandboxes:

1. Policymakers should strive to develop mechanisms for **cross-border sandbox recognition** or, at least, alignment in evaluation approaches and standards. This will help extend the value of sandbox experimentation and reduce duplication of efforts.

2. Policymakers should consider complementary investments in outreach, capacity building, and partnerships with **innovation hubs**, **technical universities** and **start-up incubators**, to help develop a more diverse and capable pipeline of sandbox participants.

3. Policymakers should **clearly communicate expectations around product maturity, governance safeguards**, and **provide well-defined terms early on** to create the conditions for effective collaboration during sandbox execution.

4. Strengthening the conditions for **safe, supervised real-world testing** is critical when preparing the execution of a sandbox advertised as such. However, data alone can sometimes not be enough. Value particularly for start-ups increases when data is combined with **compute, expert input and mentorship**.

5. Producing and sharing publicly post-sandbox outputs, such as **toolkits**, **policy recommendations and testing methodologies**, while respecting confidentiality constraints, **allows other actors to benefit from the sandbox's findings**, and highlights how sandboxes can contribute to **evidence-based approaches to AI governance**.

Recommendations for businesses

The AI Regulatory Sandbox Business Participation Checklist (Annex I) is a practical guide for businesses considering whether to participate in an AI regulatory sandbox. To be used as a conversation starter with a board, a practical guide for in-house policy teams or a sandbox introduction guide for a start-up or SME. This guide provides a series of recommendations for those considering or preparing to participate in an AI regulatory sandbox.

Looking ahead

Ultimately, the impact of AI sandboxes will depend on the ability of both public and private actors to move beyond fragmented approaches and engage with sandboxes as shared infrastructures for learning and coordination.

For policymakers, this means designing sandboxes that are inclusive, transparent, and responsive to the realities of AI systems as interconnected socio-technical ecosystems. For businesses, it means approaching sandbox engagement not only as a compliance or innovation exercise, but as a strategic opportunity to shape emerging standards, strengthen governance practices, and position themselves as trustworthy within AI markets.

Realizing this potential also requires broadening who sits at the table. AI sandboxes have largely been structured around business-to-government dynamics, but communities most affected by AI systems (e.g. civil society organizations, advocacy groups, researchers, and end users) bring perspectives that neither regulators nor industry can substitute. Future work should explore how sandboxes can be designed to meaningfully incorporate civil society as active participants, not merely as consultees or oppositional critiques,[5] ensuring that the evidence and standards they generate reflect a wider range of values, risks, and lived experiences.

[5] Datasphere Initiative (2026), Sandboxes for DPI: Co-creating the blocks of digital trust, Datasphere Initiative.

Introduction

Artificial intelligence (AI) is reshaping business models, value chains, and competitive dynamics across sectors globally.[6] Companies face growing pressure to adopt AI tools to enhance productivity, personalize services, reduce costs, and unlock new revenue streams. At the same time, policymakers are assessing how and whether to advance new regulatory frameworks to address AI-related risks,[7] including safety, accountability, data protection, competition, workforce development[8] and fundamental rights, in ways that would enable new opportunities for economic growth.

The dual pressure to innovate rapidly while navigating evolving and uncertain regulatory environments creates an urgent need for agile governance mechanisms that can support experimentation and modernize regulatory capabilities without compromising public trust. **Sandboxes** have emerged as one such mechanism: structured environments where businesses, regulators, and other stakeholders can test technologies, governance approaches, and safeguards in a controlled and collaborative setting.[9]

For companies, participation in AI regulatory sandboxes[10] is beginning to carry signaling value, almost like a "badge of honor",[11] by offering a way to demonstrate responsible AI practices, strengthen trust with regulators and users, and position a company or product competitively in emerging markets. When regulators limit business participation in sandboxes, questions are being raised around fairness in market access, particularly in instances where sandbox participation enables temporary regulatory flexibility or privileged insight into future policy directions.[12]

AI sandboxes are not only regulatory experiments - an increasing number of operational and hybrid models are opening new roles for the private sector as testing providers or operators. This creates a new dynamic in which AI sandboxes are not only governance tools, but also arenas of competitive positioning and strategic engagement for businesses.

---

6 Climent R., Haftor D., Staniewski M. (2024), AI-enabled business models for competitive advantage, ScienceDirect.

7 Mind Foundry (2026), AI Regulations around the World - 2026.

8 Mehta, N. (2026). The AI-driven workforce is here. How should your industry transform itself? World Economic Forum.

9 Datasphere Initiative (2026), Sandboxes for DPI: Co-creating the blocks of digital trust, Datasphere Initiative.

10 The Datasphere Initiative classifies sandboxes into three categories: regulatory, operational, and hybrid, according to the primary objectives of the testing environment. For further details, see the report Sandboxes for DPI.

11 Tech for Good Institute (2024), Sandbox To Society: Fostering Innovation in Southeast Asia, Tech for Good Institute.

12 Tech for Good Institute (2024), Sandbox To Society: Fostering Innovation in Southeast Asia, Tech for Good Institute.

This report expands on the research undertaken in the Datasphere Initiative's report *Sandboxes for AI: Tools for a new frontier*[13] by focusing specifically on **how businesses are engaging in AI sandboxes and the opportunities and learnings from such engagements**. While most research on AI sandboxes to date has focused on their design and deployment through the lens of the public sector, this report explores the private sector value that can be derived from participation in these initiatives and the roles businesses of all sizes can take up. The report analyzes the types of companies and sectors where AI sandboxes are gauging most interest and provides recommendations for public officials looking to attract companies to participate in their AI regulatory sandboxes. It also offers insights for the private sector considering whether and how to use sandboxes to advance their AI development or deployment ambitions.

Through case studies, policy recommendations and analysis of **90 AI sandboxes** worldwide, the report highlights how the private sector is taking up several emerging roles in AI sandboxes as participants, technical providers and operators/hosts. These roles vary depending on company size (e.g., start-up, SME, multinational), sector, and role in the AI value chain (e.g., AI developers, sectoral deployers, infrastructure providers). "Business engagement" in AI sandboxes is hence not monolithic, and instead encompasses a spectrum of incentives, responsibilities, and governance implications.

Definitions

Building on the definition introduced by the Datasphere Initiative in the *Sandboxes for Data report* (2022),[14] and updated in the recent report *Sandboxes for Digital Public Infrastructure* (2026)[15] the Datasphere Initiative defines a **sandbox** as:

> ***"a controlled learning environment designed for structured experimentation under defined governance frameworks, timeframes, and built-in safeguards to support iterative, multi-actor collaboration and evidence-based decision-making."***

[13] Datasphere Initiative (2025), Sandboxes for AI: Tools for a new frontier, Datasphere Initiative.

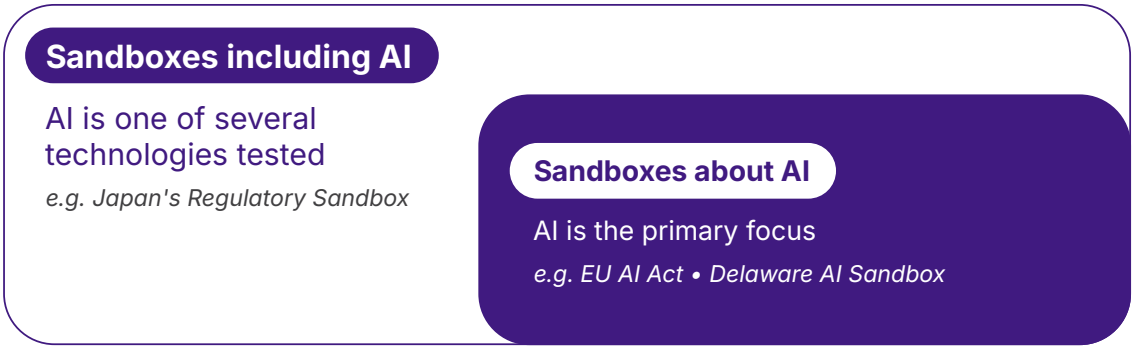
[14] In 2022 the Datasphere Initiative defined sandboxes as "safe spaces to test new technologies and practices against regulatory frameworks or experiment with innovative uses and means of governing data". Since then, the concept has evolved, which merited a new updated definition.

[15] Datasphere Initiative (2026), Sandboxes for DPI: Co-creating the blocks of digital trust, Datasphere Initiative.

Building on this general definition, and recognizing the distinct characteristics, risks and governance challenges associated with the rapid growth and deployment of artificial intelligence, this report defines an **AI sandbox** as:

> ***"a controlled learning environment in which AI systems, use cases, or related governance approaches are tested under defined conditions, timeframes, and safeguards, enabling iterative experimentation, evidence generation, and shared learning among multiple stakeholders to inform both innovation and governance."***

For the purposes of this report, the term "AI sandboxes" is used as an umbrella category encompassing all sandbox initiatives that involve AI in some capacity. Within this broader category, an important distinction is found between sandboxes **including** AI and sandboxes **about** AI.



Sandboxes including AI are a **broad category of sandbox initiatives in which AI is one of the technologies within the testing environment, but it is not necessarily the primary or only object of experimentation**. For example, Japan's Regulatory Sandbox (New Technology Testing Program) led by the Secretariat of Japan's Growth Strategy Headquarters, Cabinet Secretariat, includes a range of technologies such as Blockchain, Privacy Enhancing Technologies (PETs), Robotics & Autonomous Systems, as well as AI. It also combines a variety of domains from urban development, finance, agriculture education and energy among others.[16]

[16] Cabinet Secretariat, Government of Japan, Regulatory Sandbox.

Sandboxes about AI refer to **initiatives explicitly designed to focus on AI, where AI systems, use cases, or governance frameworks constitute the primary object of experimentation**. For example, the European Union's AI Act, requires member states to establish AI regulatory sandboxes to support innovation while ensuring compliance with the new regulatory framework.[17] At a local level in the United States, the Delaware AI Sandbox aims to create a controlled testing ground where specifically AI technologies can be safely developed and deployed across high-impact sectors, including corporate governance, biotechnology, healthcare, chemicals, and financial services.[18]

Unless otherwise specified, the reflections and insights presented in this report apply across AI sandboxes, comprising both sandboxes including AI and sandboxes about AI.[19]

Methodology

This report draws on a range of complementary research to produce a comprehensive picture of the role and value of businesses in AI sandboxes globally. The mapping updates the 2025 identification of 31 AI sandboxes to an updated count of 90 AI sandboxes in 39 countries, by building on the Datasphere Initiative's **Sandbox Explorer**, a living and growing database of 263 catalogued sandboxes worldwide.[20] Case studies were selected from across this landscape.

The report draws on insights from the Global Sandboxes Forum (GSF), which comprises policymakers, innovators and academia, whose knowledge spans sandbox design and governance across multiple jurisdictions, and a GSF insights session whose findings informed subsequent iterations of this work.[21] Broader desk research on the global status of AI sandboxes provides additional context on emerging trends and patterns in private sector engagement.

[17] EU Artificial Intelligence Act (2024), Article 57: AI Regulatory Sandboxes, European Union.

[18] Delaware.gov (2025), Delaware Launches Bold AI Sandbox Initiative, Cementing Its Role as a National Leader in Responsible Tech Innovation, Delaware News.

[19] Initiatives which do not expressly call themselves a "sandbox" but reflect the Datasphere Initiative definitions have been included in this report.

[20] Note: The number of sandboxes reflected in this report corresponds to those mapped by the Datasphere Initiative's research team as of July 2, 2026. The Datasphere Initiative plans to launch an online platform "The Sandbox Explorer" with its global sandbox mapping by the end of the year, and this report provides a sneak peak of its latest data on AI sandboxes.

[21] Datasphere Initiative (2026). Datasphere Initiative holds session to discuss the roles of the private sector in AI sandboxes, Datasphere Initiative.

Box 1. Types of businesses considered in this report

This report is intended to be relevant to all types of businesses that may engage with AI sandboxes. As there is no single universally accepted classification of business types, the report adopts a pragmatic approach based on commonly used definitions from trusted sources such as Eurostat,[22] the OECD,[23] and legal frameworks in several jurisdictions (e.g., the EU,[24] Brazil,[25] India,[26] Kenya[27] and Spain[28]).

The following business categories are considered:

- **Startups:** Recently established companies — generally not older than 5–10 years — with relatively low annual gross revenue (typically below approximately USD 3 million). These companies often rely on emerging technologies, such as artificial intelligence or blockchain, to develop and scale innovative or disruptive products or services. A "startup" is not a classification based on firm size, and such companies may in principle vary significantly in scale, although in practice they are most commonly small and medium-sized enterprises (SMEs).
- **Small and Medium-Sized Enterprises (SMEs):** Businesses employing fewer than 250 persons. They can be further subdivided into: (i) micro-enterprises: fewer than 10 employees; (ii) small enterprises: 10–49 employees; (iii) medium-sized enterprises: 50–249 employees.
- **Large enterprises:** Businesses employing 250 or more persons.
- **Multinational enterprises (MNEs):** Enterprises that produce goods or deliver services in more than one country, often operating through subsidiaries or branches across multiple jurisdictions.

With this report, the Datasphere Initiative aims to support the public and private sectors as they seek to leverage AI sandboxes for responsible innovation. While not the focus of this report, civil society and academia are also important stakeholders in AI sandbox design and deployment, as argued in the Datasphere Initiative's report *Sandboxes for AI: Tools for a new frontier* (2025). It is acknowledged, however, that further research and understanding of how to support their contributions is necessary to ensure AI regulatory and technical experimentation is safe, trustworthy and for the benefit of all.[29]

[22] Eurostat (n.d), Statistics Explained: Glossary, European Union.

[23] OECD Secretariat (2026), Structural business statistics by size class and economic activity, OECD.

[24] Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs (n.d), SME Definition, European Commission.

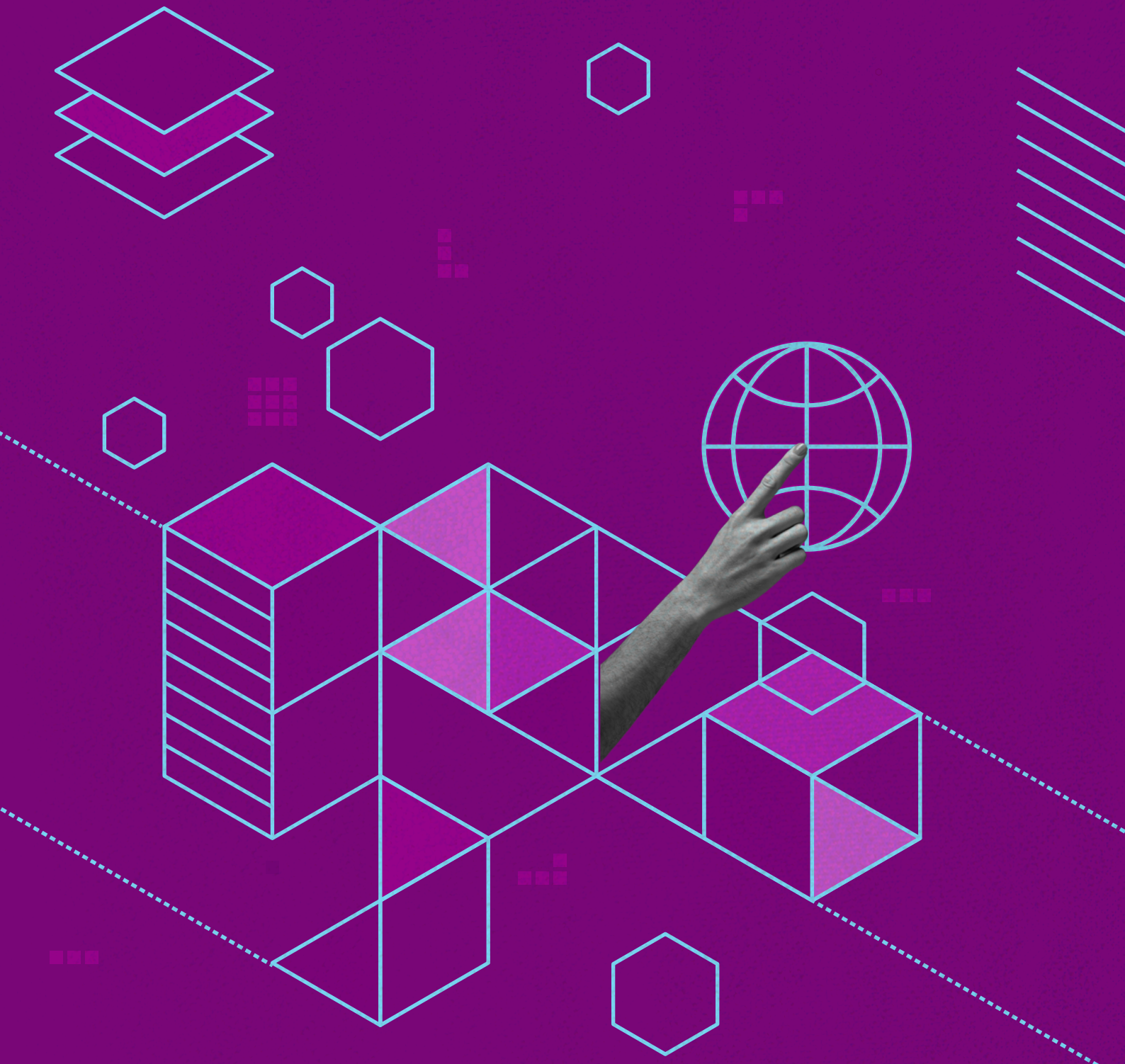
[25] General Secretariat, Sub-Chief of Legal Affairs (2006), Legal Framework for Startups and Innovative Entrepreneurship, Republic of Republic.

[26] Ministry of Commerce and Industry (n.d), Is Your Company A Startup? Government of India.

[27] The Senate (2022), The Startup Bill, 2022, Government of Kenya.

[28] Official Gazette (BOE) of Spain. Ley 28/2022.

[29] The Datasphere Initiative plans to cover the engagement of other stakeholders in sandbox design in subsequent reports of this nature.



Global overview of AI Sandboxes

Quotes from consulted stakeholders

“AI is very clearly not just for highly specialized expertise teams anymore. It is a lot more available now than it was five or six years ago."

"It comes down to access, enablement, and guardrails. Providing a neutral environment where everybody can meet and actually build.”

"Sandboxes [...] remove the heavy capital expenditure barriers typically associated with training large-scale models.”

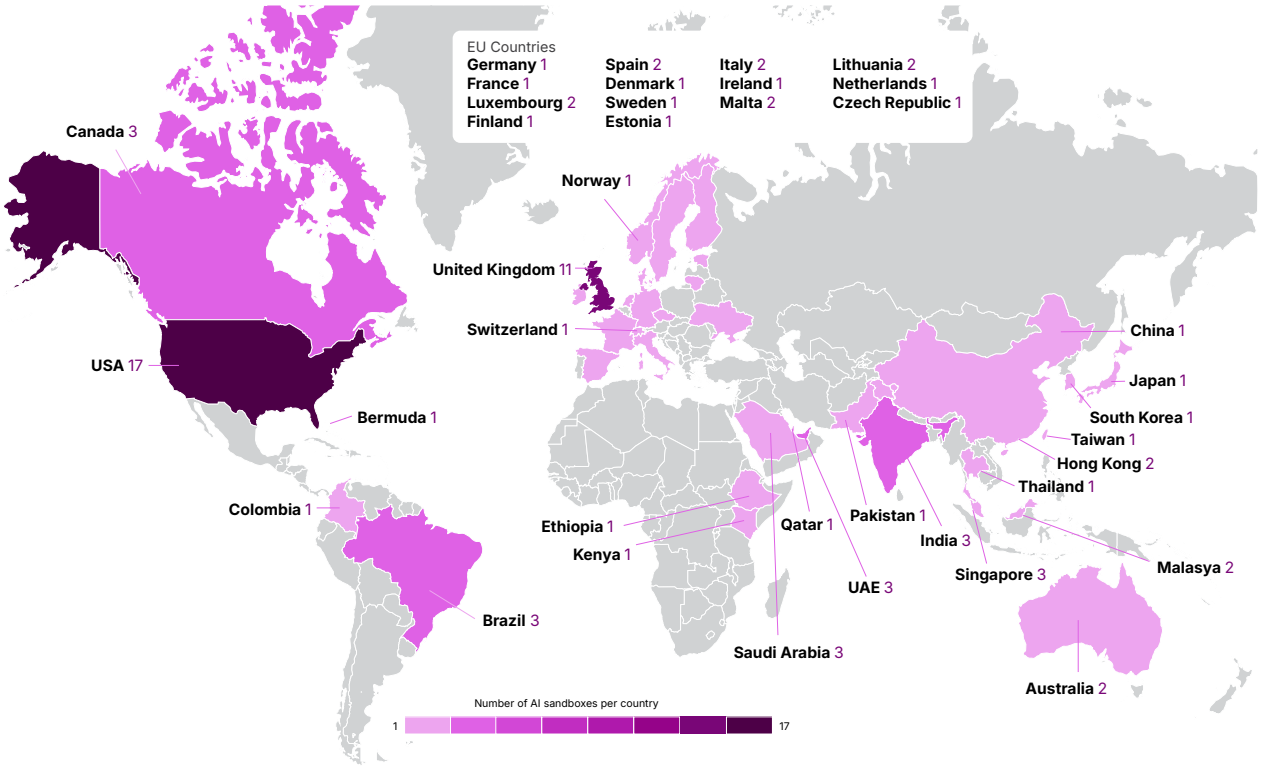
“If the goal is to help shape how AI is governed in your sector, sandboxes become a natural space to be present.”

“I'd love to get to a phase where different regulators, different governments and different industry bodies around the world would recognize the results of one single sandbox.”

From their earliest uses in financial regulation to their expansion across data, AI, and emerging technologies, sandboxes continue to evolve. Their variation reflects differences in legal traditions, regulatory cultures, institutional capacity, and societal expectations around risk, trust, and collaboration. In some contexts, AI sandboxes are formal regulatory instruments embedded in legislation and supervision frameworks; in others, they function as collaborative testbeds, policy pilots, or learning environments convened by public agencies, the private sector, and occasionally civil society, or multi-stakeholder partnerships. This chapter presents a snapshot of AI sandboxes world-wide and presents the types of sandbox models that are being used across countries.

Since the publication of *Sandboxes for AI: Tools for a New Frontier*[30] in February 2025, the global sandbox ecosystem continued to expand. **The Datasphere's mapping now identifies 263 sandboxes in 93 countries, of which 90 are AI sandboxes across 39 countries** (see Figure 1 for a global mapping of AI sandboxes).[31]

Figure 1. World Map of AI Sandboxes



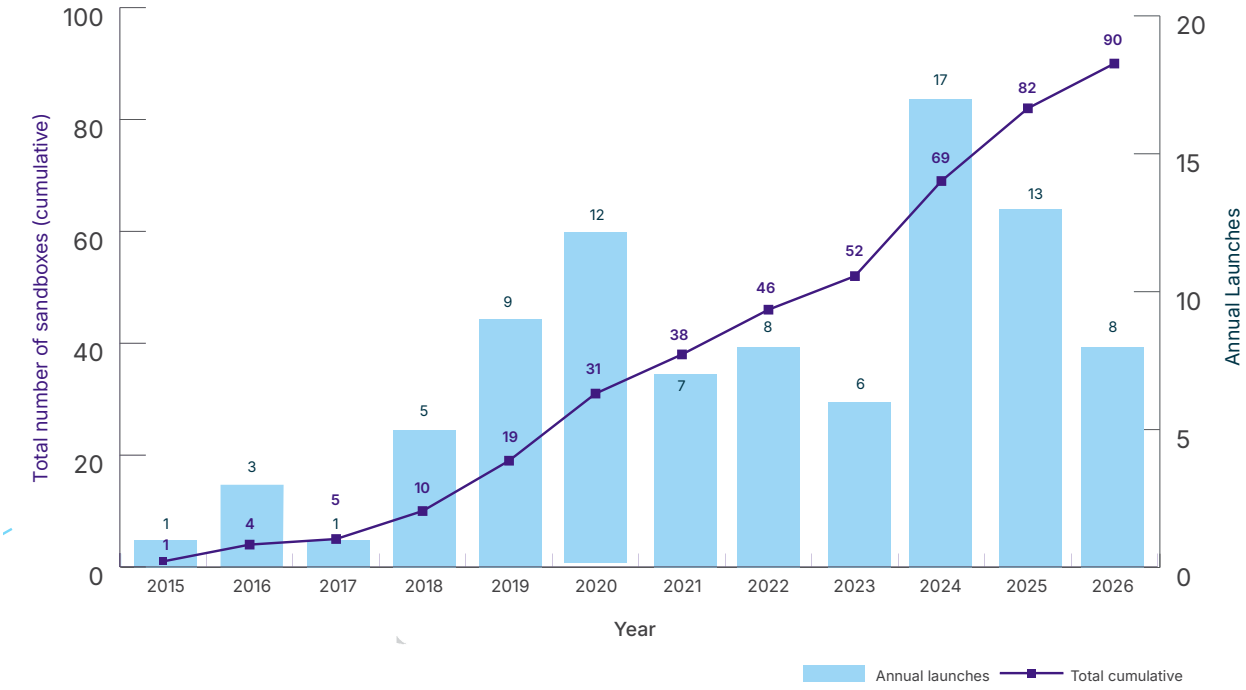
Note: This map does not show sandboxes that are multi country

[30] Datasphere Initiative (2025), Sandboxes for AI: Tools for a new frontier, Datasphere Initiative.

[31] The Datasphere Initiative plans to launch the Sandbox Explorer a global sandbox mapping, by the end of 2026, this report provides a sneak peak of its latest data on AI sandboxes

As illustrated in Figure 2, the number of identified AI sandboxes has grown steadily over the past decade. The first AI sandbox was launched in 2015,[32] followed by three in 2016, one in 2017, five in 2018, nine in 2019, twelve in 2020, seven in 2021, eight in 2022, six in 2023, seventeen in 2024, thirteen in 2025, and eight by May 2026. The cumulative growth curve shows a total of 90 identified AI sandboxes as of May 2026, reflecting the increasing institutionalization of AI sandboxes as mechanisms for governance and innovation worldwide.

Figure 2. Annual AI Sandbox Launches and Cumulative Growth (2015– 2026)



Source: Datasphere Initiative (2026).

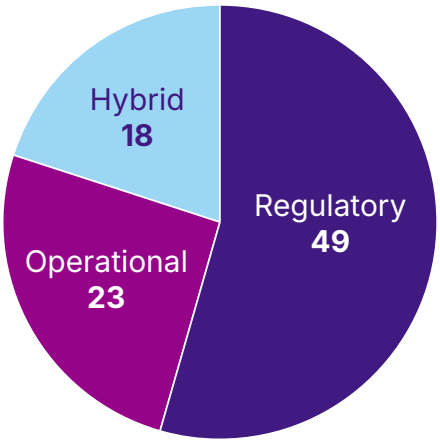
Note: The Datasphere Initiative classifies AI sandboxes as controlled learning environments in which AI systems, use cases, or related governance approaches are tested under defined conditions, timeframes, and safeguards to enable iterative experimentation, evidence generation, and shared learning among multiple stakeholders. The term AI sandboxes is used as an umbrella category encompassing both sandboxes including AI and sandboxes about AI. Sandboxes including AI refer to all sandbox initiatives where AI systems or use cases are tested, including broader sectoral or technology-agnostic sandboxes where AI is one of multiple technologies under experimentation. Sandboxes about AI refer to a subset of these initiatives specifically designed to focus on AI systems, use cases, or AI governance approaches as the primary object of experimentation. This figure maps the growth of all AI sandboxes, encompassing both categories.

[32] The sandbox mapped from 2015 is Precision FDA. This is a secure, collaborative, cloud-based high-performance computing environment that was launched by the U.S. Food and Drug Administration (FDA) to facilitate the collection, analysis, and application of data and new tools to support its mission. The platform offers collaborative opportunities, capabilities, and initiatives to help inform regulatory science, speed the Agency's understanding of evolving science, and advance the ethical and responsible use of AI to support the work of FDA regulators and scientists. The initiative was launched in 2015. While the initiative does not explicitly call itself an "AI sandbox", its description reflects the Datasphere Initiative's definition of sandboxes including AI and has thus been included in this mapping and analysis. More information see https://precision.fda.gov/about.

Beyond their growth over the last decade, AI sandboxes are also becoming more institutionally and operationally diverse. While many initiatives continue to be led by governments and regulators, the innovation ecosystems across regions often involve universities, research institutes, technology providers, startups, and other private sector actors. This reflects a broader shift in how sandboxes are being used: not only as tools for regulatory learning and compliance, but also as collaborative environments for technical testing, infrastructure access, and ecosystem building. For businesses, these evolving models create new incentives and opportunities to engage with regulators, access technical resources, reduce barriers to experimentation, and shape emerging AI governance approaches.

The data collected by the Datasphere Initiative shows that the sample of AI sandboxes identified remain predominantly regulatory in nature, with 49 of the 90 identified AI sandboxes classified as regulatory, compared to 23 operational and 18 hybrid models. This suggests that governments continue to prioritize sandboxes as tools for regulatory learning and risk management, while the use of hybrid and operational sandboxes reflects interest in supporting technical testing, infrastructure access, and real-world experimentation alongside regulatory oversight. It can also mean that other types of sandboxes, such as operational ones, may not be as publicized or publicly documented as regulatory ones - falling typically as internal exercises, by corporations or public administration bodies.

Figure 3. Types of AI Sandboxes (2015-2026)



Source: Datasphere Initiative (2026).

Note: It should be noted that the category of "hybrid sandboxes" adopted in this study follows the classification proposed by the Datasphere Initiative, which identifies sandboxes combining regulatory supervision with technical support, infrastructure, or operational testing environments. In practice, however, some sandbox coordinators may still describe these initiatives simply as "regulatory sandboxes," even when they incorporate elements that the Datasphere Initiative would classify as hybrid.

Understanding the different types of AI sandboxes is therefore crucial for companies navigating rapidly evolving AI markets and innovation environments. AI sandboxes can be classified based on their primary objectives and design, which shape the type of experimentation they enable and the value they generate for participants. Three types of AI sandboxes can be identified: regulatory, operational, and hybrid.[33]

[33] Datasphere Initiative (2022), Sandboxes for data: creating spaces for agile solutions across borders, Datasphere Initiative.

Regulatory AI sandboxes

A sandbox centered on regulatory learning or compliance, designed to generate evidence that informs existing or future rules, policies, standards, and guidance as they relate to AI.

Regulatory sandboxes are often coordinated by a regulatory authority or another public entity - such as a ministry, agency or a municipality - bringing together multiple stakeholders (e.g., companies, public sector actors, and in some cases academia and civil society) to experiment with innovations at different stages of maturity, adopting incentives for participation such as regulatory flexibility (e.g. waivers, temporary licenses, or derogations) or dialogue with public authorities. Operating under a defined governance, testing plan and built-in safeguards, regulatory sandboxes can have several goals, such as fostering innovation, enhancing safety, facilitating market access, and protecting human rights.

Operational AI sandboxes

A sandbox that provides access to data, software or infrastructure to enable the testing, validation, and improvement of AI standards or technical aspects of AI products, services, or processes (e.g., feasibility, scalability, interoperability, efficiency, or functionality), under real or simulated conditions.

Operational sandboxes can be coordinated by any entity - and support experimentation with data or any technology across different stages of maturity, from early design to testing and validation, and under local, national, or multi-country contexts.

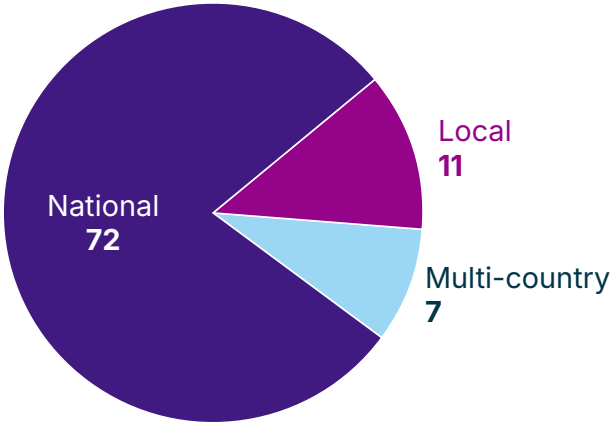
Some operational sandboxes are similar to testing environments that have been implemented by organizations such as the National Institute of Standards and Technology (NIST) in the United States, especially for conformance and interoperability testing when technical standards exist. For AI, as these standards do not yet exist, operational sandboxes could be viewed as precursors to these more formal environments.

Hybrid AI sandboxes

A sandbox that combines elements of both regulatory and operational approaches. These models allow stakeholders to both test technical aspects and to engage stakeholders in dialogues about regulation and governance, while providing some form of access to data, infrastructure, or shared technical environments.

Hybrid sandboxes should be understood as existing along a spectrum: in some cases, the emphasis lies primarily on operational experimentation, while in others regulatory guidance plays a more prominent role alongside technical testing. What characterizes a sandbox as hybrid is the presence of both dimensions, regardless of how they are weighted.

Figure 4. Governance levels of AI Sandboxes (2015-2026)



AI sandboxes can operate at different governance levels, each with distinct implications for experimentation and scaling. **National** sandboxes often focus on aligning innovation with domestic regulatory frameworks, while sub-national initiatives may provide more targeted environments for localized experimentation.

For example, at the **local** level, the Canton of Zurich AI Innovation Sandbox was established to provide a testing environment for innovative AI technologies. Launched in 2021 with a formal call for projects in March 2022, the sandbox functions as a collaborative platform, bringing together public administrations, private companies (including startups, SMEs, and large enterprises), and research institutions to address technological, regulatory, and social challenges associated with AI implementation. It enables companies to test and develop AI solutions within a clearly defined and supportive framework, while accessing regulatory expertise and novel data sources, which are often key barriers to innovation.[34]

Sandboxes can also operate at a **multi-country** level, including testing in more than one country or jurisdiction or allowing more than one country to participate in the sandbox program. For example, the Asian Development Bank's Digital Innovation Sandbox Program is open to technology companies, start-ups, and academic institutions across East Asia and the Pacific, South Asia and Central Asia to test innovative solutions related to various emerging technologies.[35] In this context, multi-country sandboxes also enable cross-border learning and experimentation. However, multi-country participation does not necessarily make a sandbox cross-border. While multi-country sandboxes may involve participants from different jurisdictions operating or experimenting under a common program, cross-border

[34] Smit M. (2025), Switzerland - Zurich - AI Innovation Sandbox, Regulations.ai

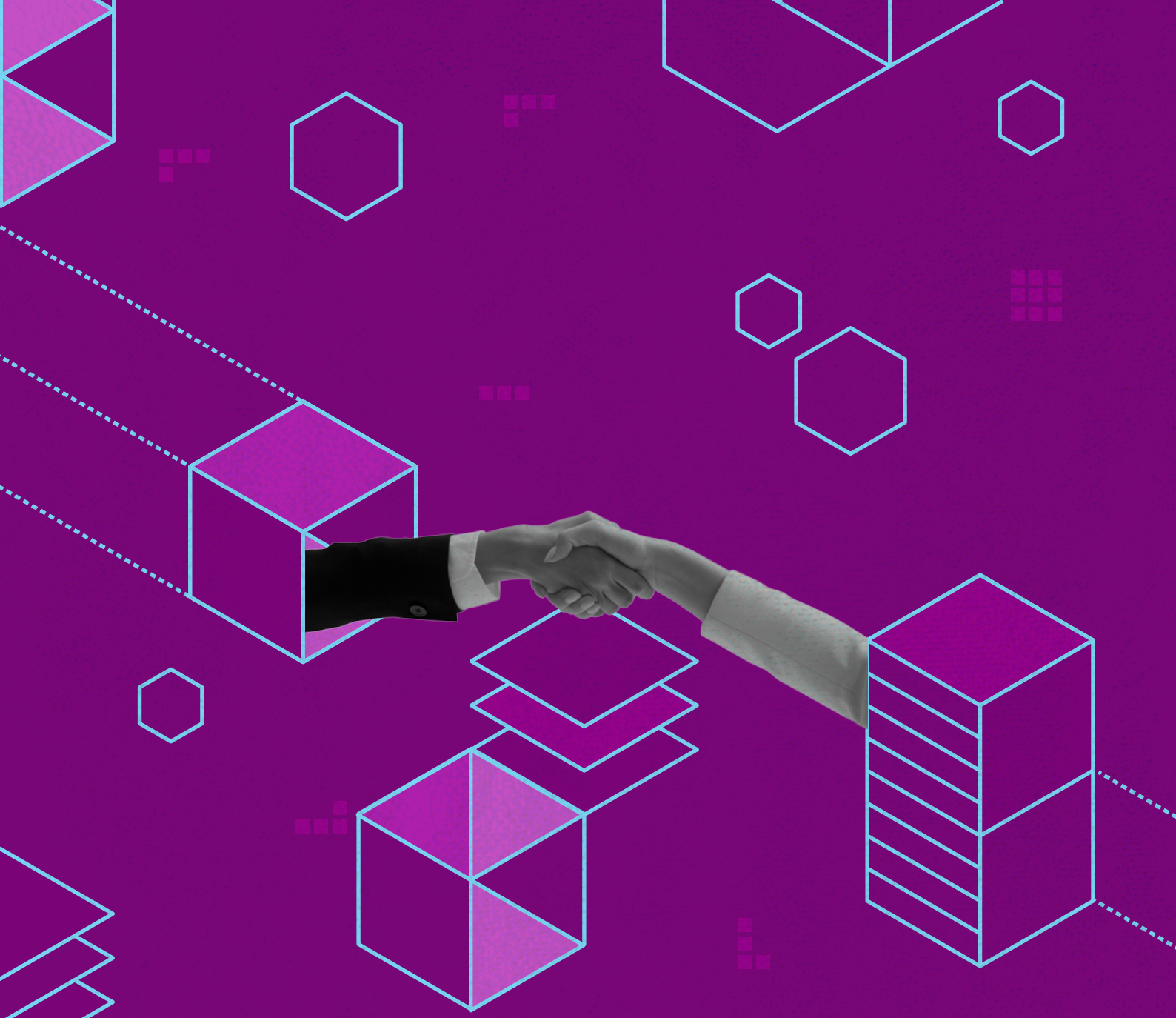
[35] Asian Development Bank (n.d.) Digital Innovation Sandbox Engagement, Asian Development Bank.

sandboxes typically entail some form of coordination between regulators or authorities across jurisdictions, including joint testing, information sharing, mutual recognition, or aligned supervisory approaches.

Cross-border AI sandboxes could add significant value for businesses and address risks and opportunities of AI innovation and regulatory uncertainty that is borderless. Companies scaling internationally must navigate overlapping regulatory frameworks, divergent standards, and inconsistent supervisory expectations, which can increase compliance costs and delay market entry. Cross-border sandboxes offer a mechanism for coordinated engagement with multiple regulators, enabling firms to test AI systems and governance approaches in parallel across markets. Cross-border experimentation may also help align technical testing methodologies, assurance processes, or certification schemes, contributing to more coherent global AI governance ecosystems. This can reduce duplicative processes, clarify expectations early, and support more predictable multi-market deployment strategies. While not focused on AI, an example of a cross-border sandbox under development for emerging technologies is the US/UK Crypto sandbox.[36] Industry stakeholders including start-ups, SMEs, and MNEs consistently provide feedback that cross-border sandboxes that unlock access to multiple markets at once would strongly incentivize participation. As AI governance frameworks mature globally, multi-level and cross-border sandboxes may evolve from experimental initiatives into strategic tools for regulatory cooperation, helping to bridge domestic innovation ecosystems with international markets while reinforcing safety, trust, and accountability. For example the UK-Singapore AI-in-Finance Partnership is a strategic collaboration between the Monetary Authority of Singapore (MAS) and the UK Financial Conduct Authority (FCA) including joint testing environments and regulatory sandboxes across both jurisdictions.[37]

[36] Coin World-AI Agent (2025), U.S.-UK Crypto Regulatory Sandbox Aims to Boost Cross-Border Innovation, ainvest.com.

[37] PathFin.ai (2026). PathFin.ai Programme and the UK-SG AI in Finance Partnership.



The role of the private sector in AI sandboxes

Quotes from consulted stakeholders

"Sandboxes cannot just be a side hustle that the companies do, it requires a dedicated team, a dedicated effort."

“A true sandbox experience for us was when we had the data, we had the compute, and we had the mentors, the industry advisors and the experts that were made available to us.”

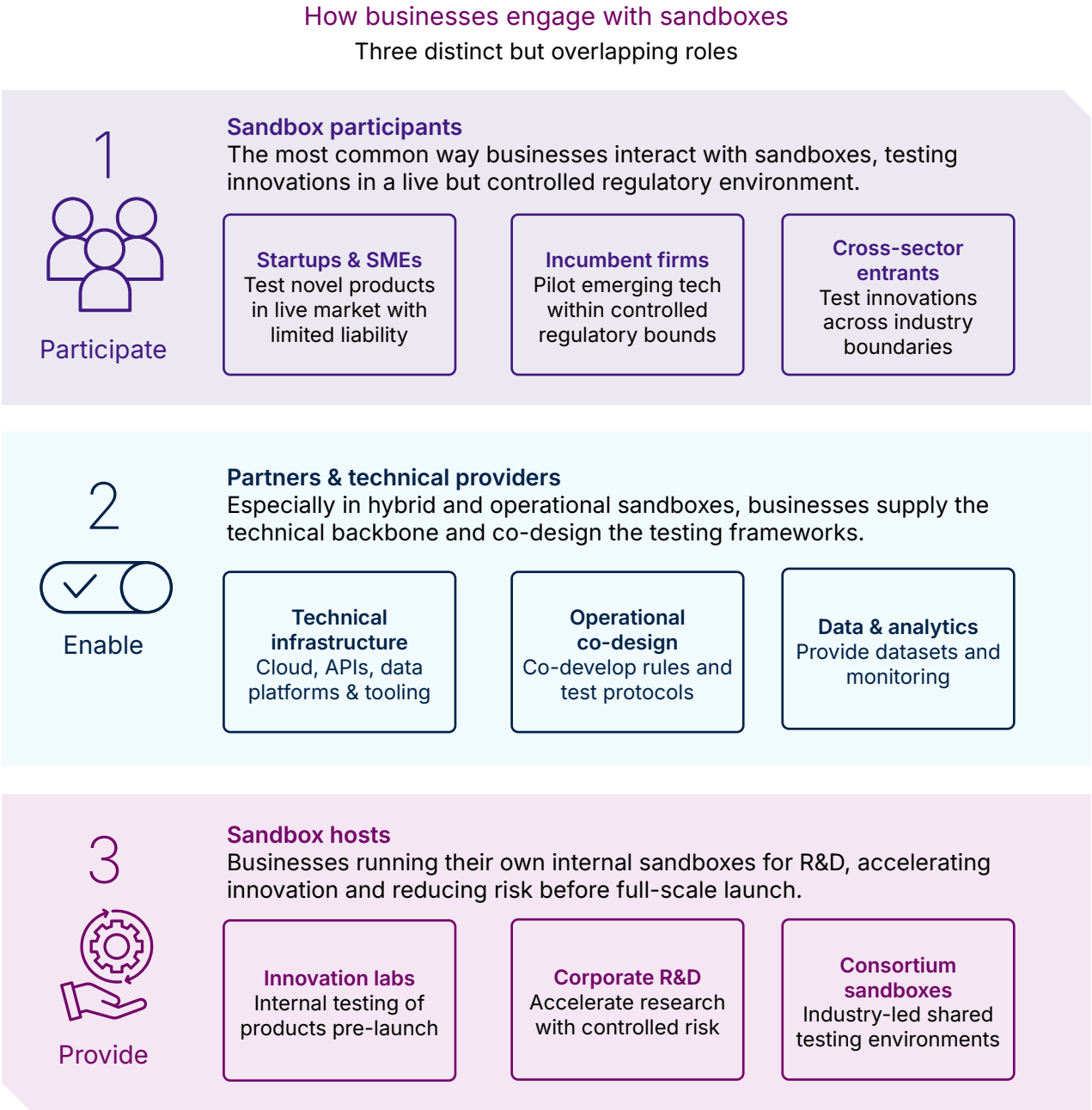
“As a multinational company, it might be challenging to partner with other companies. Environments like sandboxes allow these partnerships for brainstorming and coming up with ideas together.”

"A company needs to go into a sandbox knowing that it's worth it, that they're complying with the whole range of different laws."

The role of the private sector in an AI sandbox depends on the type of company and type of sandbox. It can also vary depending on a company's position in the AI value chain. The value proposition and incentives for a large multinational technology provider engaging in an AI regulatory or hybrid sandbox will differ significantly from those of a start-up or SME. Company size, sector, market position, and technical capacity all shape how firms perceive risk, opportunity, and strategic advantage of AI sandboxes. This chapter outlines the different private sector roles in AI sandboxes, supported by concrete examples.

As depicted in Figure 5, across different AI sandbox models (regulatory, hybrid, operational), business engagement can be understood through three core roles: **participants**, **technical providers** and **sandbox hosts**.

Figure 5. The roles of the private sector in sandboxes



First, in regulatory sandboxes businesses can act as **participants**. In this role, companies, often startups, SMEs, or innovators, enter a regulatory sandbox to test AI systems in a controlled environment. Their primary objective is to validate products, explore use cases, and better understand regulatory or operational requirements. Participation allows them to address regulatory uncertainty, improve compliance readiness, refine their technologies before scaling, and in some cases contribute to regulatory learnings and guidance.

While in regulatory sandboxes businesses have historically and are still engaged as participants, when it comes to hybrid and operational AI sandboxes the private sector can take up other roles.

In hybrid AI sandboxes, businesses can move beyond a participant's role and directly collaborate in the design of the sandbox and contribute as a **technical provider**. In this capacity, companies contribute technical infrastructure and capabilities such as testing software, platforms, data, models, APIs, or compute resources that enable the technical experimentation within the sandbox. Technical providers enable testing possibilities by providing standardized evaluation tools, benchmarks, or validation environments to rigorously assess system performance, safety, and robustness under real-world conditions. These actors are often larger technology firms or specialized providers that help create the conditions for testing and innovation. Their role is both technical and ecosystem-oriented, as they help lower barriers to entry and expand access to high-quality tools and environments.

Box 2. Businesses as technical providers in hybrid sandboxes: the case of the Global AI Assurance Sandbox

Launched as a pilot in 2025 at the Paris Peace Forum and converted into a full ongoing sandbox in July 2025, Singapore's Global AI Assurance Sandbox[38] is a joint initiative by the AI Verify Foundation and the Infocomm Media Development Authority (IMDA). It responds to a practical gap in AI governance: while principles such as fairness, transparency, and safety are widely endorsed, many organizations lack clarity on what risks should be tested, how to technically evaluate them, and who can provide credible testing and assurance services. As a result, organizations often struggle to demonstrate with confidence that their AI systems actually meet these principles in real-world conditions.

The sandbox's objectives include:

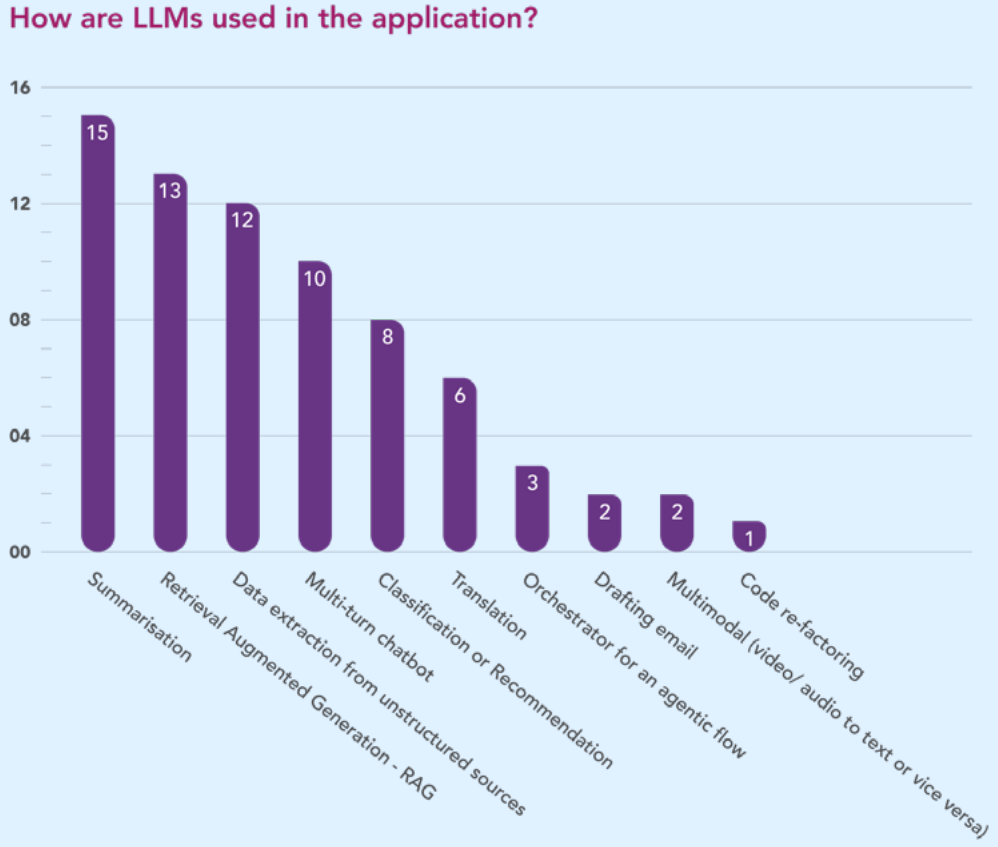
- Reduce testing-related barriers to Generative AI (GenAI) adoption through practical guidance and access to specialist testing partners.
- Provide inputs into (eventual) technical testing standards for GenAI applications.
- Support the growth of a viable AI assurance market.

[38] AI Verify Foundation (n.d), Global AI Assurance Sandbox.

Rather than functioning as a traditional regulatory sandbox, it pairs organizations that have deployed real-world AI applications with specialist external testing firms ensuring independence and credibility. Testing has focused on five common risk categories: hallucination and inaccuracy, bias in decision-making, undesirable content, data leakage, and vulnerability to adversarial prompts.[39]

As of May 2026, the Sandbox has facilitated the testing of 30 real-life Generative and Agentic AI use cases from Singapore and eleven other geographies, ensuring a strong international perspective. The exercise focused on surfacing and codifying emerging norms in the technical testing of Generative AI systems through hands-on evaluation. Spanning fourteen industries, including banking, healthcare, and technology, the Sandbox demonstrated how technical testing are already being conducted across diverse functions such as summarization, retrieval-augmented generation, data extraction, chatbots, classification, translation, agentic workflows, and code generation.

As shown in this figure from the Global AI Assurance Sandbox pilot phase main report, across the 17 applications, LLMs were used in diverse ways, prioritizing summarization, retrieval augmented generation (RAG) and data extraction from unstructured sources. Out of the 17 use cases tested, 9 were live in production, while 7 of them were in beta and/or rolled out to a limited group of users and 1 was in testing.



Source: Pilot participants and use cases - Global AI Assurance Sandbox

[39] Infocomm Media Development Authority and AI Verify (2025), Testing Real World GenAI Systems, Infocomm Media Development Authority and AI Verify.

Perhaps, the most significant insight to emerge from the Global AI Assurance's sandbox pilot was a structural perspective: testing cannot be conducted as a one-off activity. As AI applications evolve, so do their risks and many participants opted to transition to continuous evaluation pipelines as these systems evolve.[40]

Example of an AI sandbox technical provider: Resaro AI
As a technical provider in the sandbox, Resaro played a central role in translating high-level AI governance principles into concrete, testable methodologies. Their work focuses on designing end-to-end evaluation frameworks tailored to real-world, mission-critical use cases, including finance, healthcare, and public safety. This involved scoping relevant dimensions of quality, such as accuracy, safety, and compliance, calibrating test plans, selecting appropriate metrics and evaluators, and curating representative test datasets. Crucially, Resaro acts as a bridge between technical, operational, and policy stakeholders, translating complex evaluation results into clear, decision-oriented reports that enable non-technical actors to assess whether an AI system is "fit for deployment" across multiple risk dimensions.

Example of an AI sandbox participant: Tookitaki
As one of the Global AI Assurance sandbox's pilot participants, Tookitaki engaged in the sandbox to evaluate its Generative AI tool, FinMate, designed to support financial crime investigators by automatically generating structured case narratives from transaction and customer data. The tool aims to streamline the review of money laundering alerts by synthesizing relevant risk signals, contextual information, and supporting evidence into concise, actionable summaries. Within the sandbox, Tookitaki worked closely with Resaro to identify and prioritize the most critical dimensions of system performance, ensuring that the tool not only functioned technically but delivered meaningful value in real investigative workflows.

In the case of operational sandboxes, businesses can join as participants, technical providers but also take on the role of sandbox hosts or operators. Here, companies can design, manage, and offer sandbox environments themselves, sometimes as a service to other firms, governments, or innovation communities. These "sandbox-as-a-service" models position businesses as infrastructure builders and ecosystem orchestrators, shaping how experimentation happens and who can participate.

[40] Infocomm Media Development Authority and AI Verify (2025), Testing Real World GenAI Systems: Main Report, Infocomm Media Development Authority and AI Verify.

Box 3. Business as a host of an operational sandbox: the case of Sandbox AQ

SandboxAQ is a global operational sandbox company providing AI and quantum-based solutions to governments, healthcare systems, financial institutions, defense bodies, and research organizations. Originally incubated within Alphabet's Google X in 2016, it became an independent company in 2022 and operates as a Software-as-a-Service (SaaS) provider.

The sandbox focuses on four domains: post-quantum cybersecurity, quantum sensing (AQMed), quantum navigation (AQNAV), and simulation and optimization for drug and materials discovery. It enables organizations to test, validate, and deploy AI and quantum-adjacent technologies using existing infrastructure, without waiting for fully mature quantum hardware.

SandboxAQ operates through project-based engagements and licensing models, often in partnership with global systems integrators. It supports organizations in inventorying cryptographic systems, accelerating research and development timelines, testing advanced sensing devices in clinical settings, and developing navigation systems for GPS-denied environments.

The sandbox includes:

- Secure, standards-aligned infrastructure (including alignment with NIST post-quantum cryptography guidance).
- Sector-specific testing environments for cybersecurity, healthcare, defense, and scientific research.
- Access to advanced AI models, simulation capabilities, and open datasets.
- Education and capacity-building initiatives to improve institutional readiness.

Building on experimentation, deployment, and standards engagement, SandboxAQ demonstrates how operational sandboxes can function as long-term infrastructure for responsible innovation in highly regulated and high-risk sectors.

Operational sandboxes can also support companies' R&D efforts and allow clients to test and explore products and services. Several technology firms are acting as sandbox **hosts or operators**, offering 'sandbox-as-a-service' environments where others can experiment with their data, models, and compute resources (see Box 5) .

Box 4. The growing role of infrastructure providers like NVIDIA in hybrid sandbox models

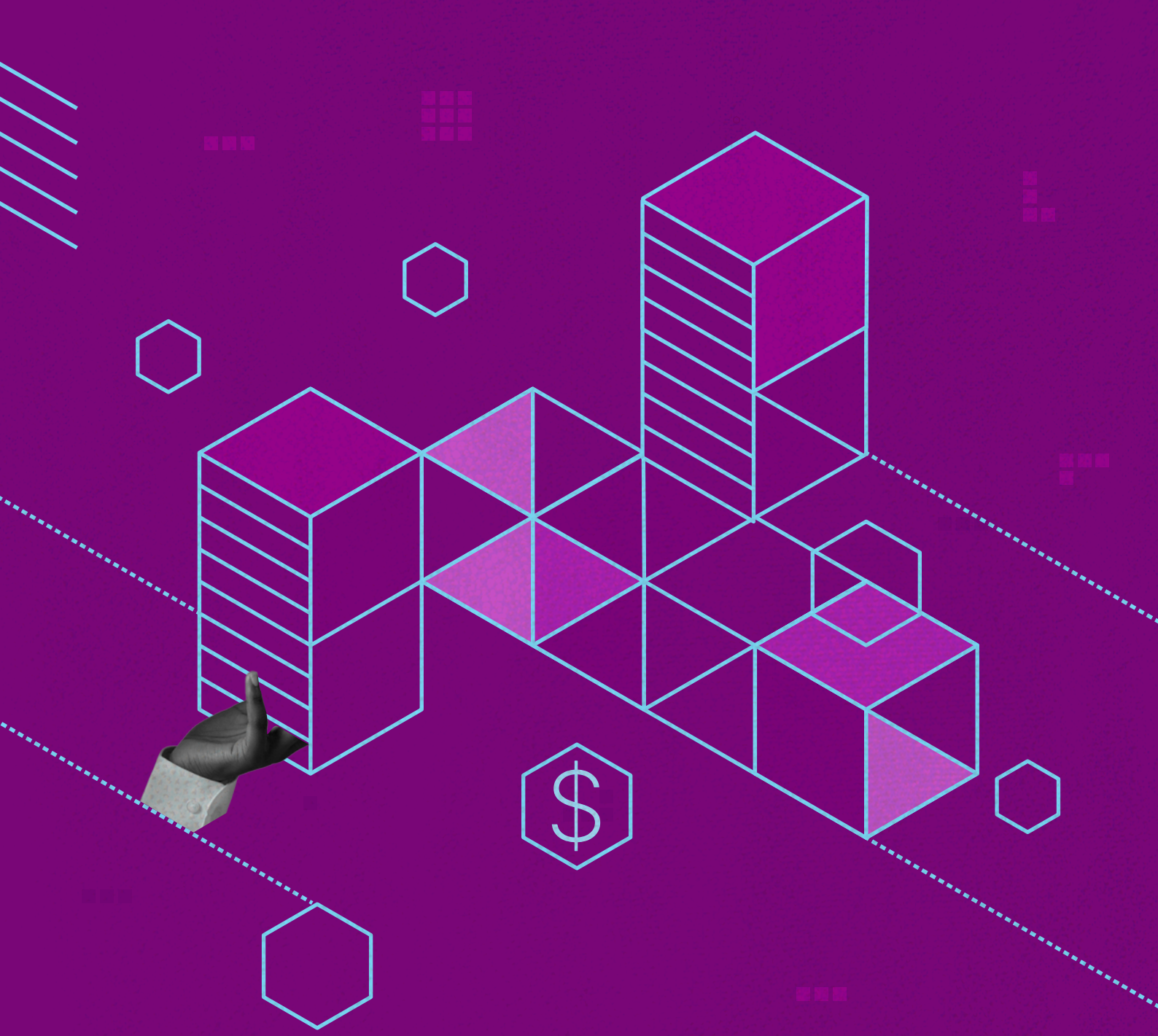
As hybrid sandboxes evolve, technical providers are playing a complementary role by supplying the compute infrastructure, software stacks, datasets, and technical environments needed to support experimentation at scale. These actors enable sandbox participants to test, train, and deploy AI systems in production-grade environments while regulators maintain oversight functions.

One example is NVIDIA's collaboration with sandbox initiatives in jurisdictions such as the United Kingdom[41] and Malaysia,[42] where the company has supported AI experimentation by providing access to GPU-accelerated compute infrastructure and scalable AI development environments. NVIDIA contributes the technical backbone that allows companies to rapidly prototype and test AI applications using open-source models, synthetic datasets, and deployable software stacks.

Beyond financial services, these partnerships also reflect a broader trend toward hybrid sandbox models where public sector oversight is combined with private sector technical capacity. This includes the provision of compute resources, AI tooling, and operational environments that many startups, regulators, and smaller firms would otherwise struggle to access independently.

[41] Financial Conduct Authority (2025). FCA allows firms to experiment with AI alongside NVIDIA, Financial Conduct Authority.

[42] Malaysian Research Accelerator for Technology and Innovation (2024). AI Sandbox launch with NVIDIA, MIRANTI.



The value of AI sandboxes for the private sector

Quotes from consulted stakeholders

"The unique expert stakeholder network that we formed as part of our sandbox really did help to expand the network for the innovators as well."

"In order for our test results to be actually predictive of how the system will behave once it's deployed in operation, we need test data to be operationally representative."

"There might be a different distinction between innovation spend and a product that is commercially viable that needs to go globally. And that includes anything from operational costs or legal costs."

"Regulatory sandboxes should not just be tools to test compliance, they should be playing a much more strategic role in informing better rulemaking, better policymaking."

The value of AI sandboxes for businesses is not uniform but varies significantly depending on the type and size of the company and the type of sandbox. This chapter explores the types of value AI sandboxes can offer businesses and shares examples of emerging models and practices.

Broadly, businesses may derive value from AI sandboxes in three interconnected ways: by reducing regulatory uncertainty and strengthening trust and legitimacy; by enabling technical experimentation, validation, and responsible scaling; and by supporting AI adoption, organizational or regulatory learning, and long-term capability-building. The table below provides a high-level summary of the value companies can derive from participating in regulatory or operational AI sandboxes. A combination could be anticipated regarding participation in a hybrid sandbox.

Table 1. Value of participating in a sandbox by business type

Type of business	Value of regulatory sandboxes	Value of operational sandboxes
All businesses	☐ Regulatory validation ☐ Enhanced business legitimacy ☐ Reduced regulatory uncertainty ☐ Reduced compliance risks ☐ Controlled pre-deployment testing ☐ Regulatory flexibility ☐ Structured engagement with regulators ☐ Visibility within the innovation ecosystem	☐ Technical validation of proofs of concept or prototypes ☐ Harmonization of technical standards ☐ Risk reduction through real-world testing ☐ Assess market viability of products
Small and Medium-Sized Enterprises (SMEs) and startups	☐ Increased investment attractiveness ☐ Accelerated path to compliant market entry ☐ Expert input and mentors ☐ Access to research advisors	☐ Access to data, infrastructure, and technical resources ☐ Technical learning
Large Enterprise	☐ Assurance for large-scale deployment ☐ Co-design of regulatory frameworks	☐ Support scaling assessments ☐ Co-design of operational frameworks and technical standards
Multinational enterprises (MNEs)	☐ Reduced cross-border regulatory uncertainty ☐ Global market alignment	☐ Cross-border testing and deployment ☐ Enhanced global legitimacy

Source: Datasphere Initiative (2026)

Notes: (1) The "values" highlighted for specific business categories are intended to reflect predominant patterns observed across the mapping. However, these examples are illustrative rather than exhaustive or exclusive, and the distinctions should not be interpreted as rigid, as many of the identified benefits and opportunities may also apply across different types of companies depending on their role, maturity, sector, and level of engagement within sandbox environments. (2) The business categories used in this table are based on a pragmatic classification by the Datasphere Initiative, drawing on commonly used definitions from international organizations and legal frameworks. They include startups (recently established, innovation-driven companies), SMEs (businesses with fewer than 250 persons), large enterprises (250 or more persons), and multinational enterprises (MNEs) producing goods or delivering services in more than one country. For sources and definitions of the types of sandboxes referenced in Table 1, refer to Box 1 in the introduction.

Regulatory clarity, compliance and trust-building

AI regulatory sandboxes create value for businesses primarily by reducing legal and compliance uncertainty while enabling closer engagement with regulators. Start-ups and early-stage firms often operate with limited capital, lean compliance teams, and high uncertainty regarding regulatory expectations. For companies developing or deploying AI, particularly in high-risk or highly regulated sectors, these environments offer a structured pathway to test systems, refine compliance approaches, and anticipate future regulatory expectations.

Data from the Organisation for Economic Co-operation and Development (OECD) underscores the strategic importance of regulatory clarity for AI investment.[43] By 2025, AI firms accounted for 61% of global venture capital investment (USD 258.7 billion), with funding increasingly concentrated in large-scale "mega-deals" and in a small number of jurisdictions. This concentration reflects both the rapid scaling of AI technologies and investor sensitivity to regulatory predictability, infrastructure capacity, and market stability.

Sandboxes could help grow domestic AI ecosystems by serving not only as regulatory learning tools but also as confidence-building mechanisms that reduce uncertainty for investors, signal governance maturity, and position local firms within globally competitive and trustworthy AI markets.

Box 5. The value of regulatory sandboxes for SMEs: the case of three companies in the Norwegian Data Protection Authority's Regulatory Sandbox for AI

The regulatory sandbox of the Norwegian Data Protection Authority has supported several SMEs in navigating complex data protection challenges while developing innovative, data-driven solutions since 2021. Some of these companies have included:

- **Secure Practice (cybersecurity & employee risk profiling).** Sandbox participant, Secure Practice sought to develop a service that profiles employees' cybersecurity risk to enable targeted training. Through the sandbox, the company worked closely with the regulator to address sensitive issues around employee monitoring and privacy. This led to strengthened privacy-by-design practices, including anonymization strategies and a robust Data Protection Impact Assessment (DPIA), ensuring that individual employees could not be directly identified from risk data.[44]

[43] Secretary-General of the OECD (2026), Policy Brief: Venture capital investments in artificial intelligence through 2025, OECD.

[44] Datatilsynet (2023). Evaluation of the Norwegian Data Protection Authority's Regulatory Sandbox for Artificial Intelligence pg. 19, Norwegian Data Protection Authority.

- **Finterai (AI for anti-money laundering).** Sandbox participant, Finterai aimed to improve banks' ability to detect money laundering using machine learning, but faced a fundamental barrier: banks cannot share transaction data due to privacy rules. In the sandbox, the company explored federated learning, allowing banks to train models collaboratively without sharing personal data. This helped clarify key regulatory questions around roles, data minimization, and security, while demonstrating a privacy-preserving technical architecture that reduces false positives and compliance burdens.[45]

- **Mobai (privacy-preserving facial recognition).** Sandbox participant, Mobai worked on developing facial recognition technology using advanced encryption techniques. Given the high-risk nature of biometric data and AI-based identification, the sandbox provided a setting to test how such systems can meet strict data protection requirements. The process supported the development of privacy-enhancing technologies (e.g., encrypted biometric processing) and helped address regulatory concerns early in the design phase.[46]

Across these cases, the sandbox delivered three core benefits:

1. **Reduced regulatory uncertainty**: SMEs gained clarity on how GDPR applies to novel AI and data use cases

2. **Improved product design:** Legal requirements were translated into concrete technical solutions (e.g., anonymization, federated learning, encryption)

3. **Lower compliance risk:** Early regulatory engagement helped avoid costly redesigns and enabled more confident scaling.

The key takeaway from these stories is precisely that for SMEs operating in high-risk data environments, regulatory sandboxes act as a bridge between innovation and compliance, enabling them to test, refine, and de-risk cutting-edge solutions that would otherwise struggle to reach deployment.

Besides compliance-related benefits, regulatory or hybrid sandboxes may also add **reputational value** for participating companies. These reputational effects are context-dependent and may change according to the type of business, regulatory environment, and maturity of the market. Participation in a sandbox can operate as a form of external validation, signaling that a company is proactively engaging with regulatory requirements, developing trustworthy technologies, and aligning itself with emerging governance standards.

[45] Datatilsynet (2023). Evaluation of the Norwegian Data Protection Authority's Regulatory Sandbox for Artificial Intelligence pg. 20, Norwegian Data Protection Authority.

[46] Datatilsynet (2023). Evaluation of the Norwegian Data Protection Authority's Regulatory Sandbox for Artificial Intelligence pg. 21, Norwegian Data Protection Authority.

For startups and SMEs, reputational gains are often closely linked to investment attractiveness. Acceptance into a regulatory sandbox may provide a form of regulatory endorsement, enhancing the credibility of participating firms and helping them attract customers and investors.[47] Sandbox participation may point to a company's willingness to move out of regulatory "grey zones" and engage proactively with compliance obligations, thereby increasing legal certainty and improving its investment appeal.[48] A report by the UK Financial Conduct Authority on its regulatory sandbox indicated that at least 40% of firms completing tests in its first cohort received investment during or shortly after participation.[49] Also, a report from European Financial Supervisory Authorities show that investment firms are also engaging in regulatory sandboxes to cooperate and engage directly with participants.[50]

There may also be reputational incentives from the expectation that participation in the sandbox contributes positively to future compliance assessments. Under the EU AI Act, competent authorities must provide sandbox participants with guidance regarding regulatory expectations and, upon request, written documentation of successfully completed activities and exit reports.[51] The Act further mandates that these reports should be "taken positively into account" during conformity assessments and market surveillance procedures, potentially accelerating compliance processes. In this sense, participation in AI regulatory sandboxes may create a formal presumption of regulatory compliance, allowing companies to benefit from the experience accumulated under regulatory supervision and from the ongoing dialogue established with competent authorities during testing phases.[52]

Another key benefit of joining regulatory or hybrid sandboxes is the possibility of obtaining a degree of **regulatory flexibility** during the experimentation process. Rather than creating "regulation-free" environments, sandboxes typically offer limited and controlled forms of legal or supervisory flexibility aimed at enabling innovation while maintaining safeguards for affected stakeholders.[53] There are different mechanisms through which this flexibility may operate, including no-enforcement letters, temporary or restricted authorizations, targeted legal derogations, and supervisory discretion in the application of rules.[54] In practice, these mechanisms may help companies test innovative products under regulatory supervision, clarify compliance expectations, and reduce uncertainty associated with emerging

[47] Allen (2019) Regulatory Sandboxes, Addressing the Global Challenges for Responsive FinTech Regulation, p. 625.

[48] Dardykina (2025) 'Is There Enough Sand in the Sandbox?, European Business Law Review, Issue 7, pp. 1083-1120.

[49] Financial Conduct Authority (2017), Regulatory Sandbox Lessons Learned Report, Financial Conduct Authority.

[50] European Supervisory Authorities (2023) Report - Update on the functioning of innovation facilitators – innovation hubs and regulatory sandboxes, ESA.

[51] Article 57(7) of the EU AI Act.

[52] Mobilio and Gianelli (2025) Legal Basis for Regulatory Sandboxes: Key Aspects for a Coherent Theoretical and Practical Framework, p. 42.

[53] Ranchordás and Vinci (2024). Regulatory Sandboxes and Innovation-Friendly Regulation: Between Collaboration and Capture.

[54] Buocz, Pfotenhauer and Eisenberger (2023). Regulatory Sandboxes in the AI Act: Reconciling Innovation and Safety?

technologies. Nevertheless, regulatory flexibility does not generally entail exemptions from liability or the removal of regulatory oversight. In a global analysis of fintech sandboxes, the World Bank observed that participants are commonly required to keep safeguards for customers and third parties, including financial capacity to address potential harms.[55] Within the European context, the EU AI Act adopts a relatively cautious approach to flexibility: Instead of broad exemptions, Article 57(12) establishes limited protections against administrative fines for participants acting in good faith and in compliance with sandbox requirements.[56] More broadly, regulatory flexibility in sandboxes depends on a clear statutory basis to ensure legitimacy, legal certainty, and compatibility with rule of law.[57]

Technical experimentation, validation and scaling

Hybrid AI sandboxes are particularly valuable for companies operating in AI contexts where technical performance and regulatory compliance are deeply intertwined. For these actors, regulatory or hybrid sandboxes can help companies reduce legal uncertainty while testing AI systems under supervisory guidance. For SMEs and start-ups entering regulated sectors, these sandboxes may provide additional benefits. They can support proof-of-concept validation and product scalability assessments, facilitate alignment with emerging regulatory frameworks, and help reduce early compliance costs. Participation may also strengthen credibility with investors and business partners, while providing access to shared data, infrastructure, and technical resources that might otherwise be prohibitively expensive.

However, data alone can sometimes not be enough. Value particularly for start-ups in hybrid AI sandboxes, can increase when data is combined with compute, expert input, realistic testing contexts, mentors and research advisors. The combination of mentors and a cohort community can enrich the experience particularly for start-ups, making the sandbox feel like a testing environment that reflects how real businesses operate.

Companies developing or deploying AI systems must often validate safety, robustness, explainability, or bias mitigation while also demonstrating alignment with evolving governance expectations. Hybrid sandbox models allow these processes to occur simultaneously. For businesses, hybrid sandboxes can reduce the gap between technical development and regulatory approval. Instead of building a product first and seeking compliance later, firms can co-design, test, and refine both technical features and governance safeguards in parallel. This integrated approach lowers redesign costs, accelerates responsible deployment, and reduces uncertainty around regulatory interpretation.

[55] World Bank Group (2020), Global Experiences from Regulatory Sandboxes, World Bank Group.

[56] Genicot and Moraes (2026) Exploring the boundaries of AI regulatory sandboxes under the AI Act: Flexibility and real-world testing.

[57] Mobilio and Gianelli (2025) Legal Basis for Regulatory Sandboxes: Key Aspects for a Coherent Theoretical and Practical Framework.

However, many regulatory or hybrid AI sandboxes operate within only one jurisdiction and sometimes one sectoral domain, arguably limiting the value for large enterprises and multinational technology firms. These companies typically manage established compliance systems and operate across multiple jurisdictions. Their interest in engaging in AI regulatory or hybrid sandboxes is often less about regulatory clarification in a single jurisdiction and more about de-risking complex AI deployments, anticipating regulatory divergence across markets, shaping implementation standards, and strengthening reputational trust.

An example of a sandbox that has attracted multinational companies is the Singapore IMDA's Privacy Enhancing Technology (PET) sandbox.[58] Meta piloted their "Interoperable Private Attribution" (IPA) proposal, asking for clarification on whether the platform (browser or mobile device vendor) would be considered to have collected, used or disclosed personal data for the generation of the attribution report, and if there were any additional safeguards required to ensure compliance with PDPA.[59] Mastercard and Tiktok also undertook testing within the IMDA sandbox.[60]

While regulatory sandboxes focus on compliance and governance, hybrid or operational sandboxes create value by enabling technical experimentation, learning, and validation. They provide businesses with access to data, infrastructure, and collaborative environments to test AI systems in practice, often before significant investments are made. For AI-core or infrastructure providers, operational sandboxes may present strategic opportunities to validate technical tools, demonstrate assurance capabilities, and position themselves as long-term ecosystem partners.

Box 6. Access to compute and data in a hybrid sandbox: the case of the UK FCA Supercharged AI Sandbox

The UK's Financial Conduct Authority (FCA) has advanced its sandbox model through the launch of its AI Supercharged Sandbox, which aims to address one of the most significant barriers to AI innovation: access to high-quality compute, scalable infrastructure, and deployable environments.[61]

Building on the FCA's Digital Sandbox,[62] operated by NayaOne,[63] the Supercharged Sandbox integrates GPU-accelerated compute, enriched datasets, and ready-to-use AI development tools into a single environment. This hybrid sandbox allows for advanced AI experimentation, enabling participants to move quickly from idea to testing without the typical delays associated with infrastructure setup. Instead of spending time configuring systems, participants can focus from the outset on experimentation, evaluation, and iteration.

[58] Infocomm Media Development Authority (2023), Privacy Enhancing Technology Sandboxes.

[59] Infocomm Media Development Authority (2023), Digital advertising in a paradigm without 3rd party cookies IMDA PET Sandbox - Meta Case Study, Infocomm Media Development Authority.

[60] Infocomm Media Development Authority (2023), Privacy Enhancing Technology Sandboxes.

[61] Financial Conduct Authority (2025), FCA allows firms to experiment with AI alongside NVIDIA, Financial Conduct Authority.

[62] Financial Conduct Authority (2020), Digital Sandbox, Financial Conduct Authority.

[63] NayaOne (2026), Inside the FCA's Supercharged Sandbox Showcase, NayaOne.

A core feature of the model is the use of NVIDIA's full-stack AI infrastructure, which supports the entire lifecycle, from data preparation and model training to deployment. GPU acceleration makes it feasible to run complex models efficiently, significantly reducing costs and development time while enabling more advanced use cases.

The sandbox also provides access to synthetic and realistic datasets and operates as a collaborative ecosystem, connecting firms with regulators and technical experts. This lowers entry barriers for smaller firms, who would otherwise not have AI testing capabilities, and supports the responsible testing of AI applications in areas such as retail finance, compliance, and wholesale markets.[64]

Importantly, the environment is designed for portability and real-world readiness. Solutions are built in production-grade conditions and can be deployed in other GPU-enabled settings with minimal adaptation, allowing teams to scale by simply increasing compute capacity. This helps bridge the common "proof-of-concept gap" and accelerates time to market.

Through its combination of compute access, data, and regulatory engagement within a single framework, the Supercharged Sandbox enables firms to move beyond prototypes toward scalable, deployable, and responsibly governed AI systems.

AI adoption, organizational learning and capability-building

Companies looking to deploy AI face growing pressure to learn and adapt quickly to this technological transformation, while simultaneously navigating uncertainty around the AI marketplace and regulatory landscape. On one hand, some research points to the potential benefits of AI with businesses reporting productivity gains and reinvesting these gains into further adoption.[65] However, opportunities are matched by equally significant risks and operational challenges. Many companies struggle to identify which AI applications are truly valuable, how to integrate them into existing systems, how to manage them centrally, and who within the organization should lead these efforts. As illustrated in practice, AI adoption is often fragmented and is characterized by unclear ownership, underutilized tools, and disconnects between leadership, technical teams, and data governance functions.[66] Companies also face material risks, including model hallucinations, bias, and unreliable outputs that can lead to flawed decision-making. These risks extend beyond technical performance to include reputational damage, privacy concerns, and longer-term organizational impacts, such as the

[64] Financial Conduct Authority (2025), FCA allows firms to experiment with AI alongside NVIDIA, Financial Conduct Authority.

[65] Henderson, J. and Smith, J. (2026), How Boards Can Lead in a World Remade by AI, Harvard Law School Forum on Corporate Governance.

[66] Austin, H. and Gregory, S, (2025), AI and the Role of the Board of Directors, Harvard Law School Forum on Corporate Governance.

erosion of entry-level roles that traditionally build future talent pipelines.[67] These risks are compounded as organizations explore agentic AI systems.[68]

Operational AI sandboxes can enable companies to test, evaluate, and iterate before making significant investments in AI systems. Rather than committing to expensive and resource-intensive deployments upfront, companies can experiment with different models, providers, and use cases in controlled environments, helping them better understand performance, risks, organizational fit and ensuring that their data is AI ready. These testing and learning environments also create opportunities for in-house teams to co-design solutions, build internal capabilities, and align technical development with governance and business objectives.

Box 7. AI Agent Sandboxes: an emerging operational model

An emerging sandbox trend for further investigation is AI Agent sandboxes. These securely isolated execution environments, take inspiration from sandboxing in the context of software, providing spaces where an agent can take actions such running code and browse pages without implicating the host system or production data.[69] Several AI agent sandbox providers have emerged in recent years[70] indicating a potential trend in the private sector providing these as operational sandbox tools. In 2025 the UK AI Security Institute released "The Inspect Sandboxing Toolkit: Scalable and secure AI agent evaluations" providing a set of guidance to accommodate a variety of agentic evaluation environments for advanced AI models, along with documentation on how to approach choosing a sandbox.[71] As explored in the 2026 International AI Safety Report, while 'sandboxing' AI agents can make it much easier to oversee and manage them, these tools cannot always be leveraged for applications where an AI system must necessarily act in the real-world.[72]

Multinational technology companies are offering operational AI sandboxes as commercial environments for prospective users to test their AI models and services, supporting access and potential investment into their own tools and AI packages. These environments allow prospective users to test models, access compute infrastructure, and experiment with pre-built tools within the providers' ecosystems. While this expands access to advanced capabilities and lowers technical barriers, it also shapes adoption pathways, often incentivizing companies to build on specific stacks and transition into longer-term use of those platforms.

---

[67] Mitchell, S. (2025), Data Governance Foundations for Boards: Governance guidance to drive innovation, Australian Institute of Company Directors.

[68] ACSC, CISA, NSA et al., (2026), Careful Adoption of Agentic AI Services; see also IMDA, Model AI Governance Framework for Agentic AI (May 2026).

[69] Pathak (2026), AI Agent Sandbox: How to Safely Run Autonomous Agents in 2026, Firecrawl.

[70] Pathak (2026), AI Agent Sandbox: How to Safely Run Autonomous Agents in 2026, Firecrawl.

[71] UK AI Security Insitute (2025), The Inspect Sandboxing Toolkit: Scalable and secure AI agent evaluations, UK AI Security Insitute.

[72] Clare & Prunkl (2026), International AI Safety Report, International AI Safety Report.

As such, these sandboxes function not only as innovation enablers but also as access roads into specific AI ecosystems, influencing both technical choices and market dynamics. One example of this "try before you integrate" model is outlined in Box 8.

Box 8. Operational sandboxes offering a "try before you integrate": the case of Google's AI Studio Sandbox

Google's AI Studio illustrates how multinational technology companies are developing operational sandboxes as commercial environments to support and simplify early-stage AI experimentation. Designed as a cloud-based development platform, AI Studio enables users to interact with Gemini, Google's multimodal AI models, through a low-code and prompt-based interface "where developers can fine-tune and evaluate AI outputs in real-time".[73]

The platform lowers barriers to entry by providing an accessible environment where users can experiment with AI in real time, including generating code, building simple applications, and testing multimodal use cases such as text, image, and video inputs. By simplifying the process of working with advanced models, Google's AI Studio enables both technical and non-technical users to explore potential applications without requiring significant upfront investment in infrastructure.

As an operational sandbox, AI Studio exemplifies a "try before you integrate" approach: firms and individuals can test ideas, assess model behavior, and refine use cases prior to embedding AI into core systems. At the same time, the platform highlights important limitations and considerations, including its experimental nature and the need for caution when handling sensitive data, as data protection and governance safeguards may not yet be fully established.

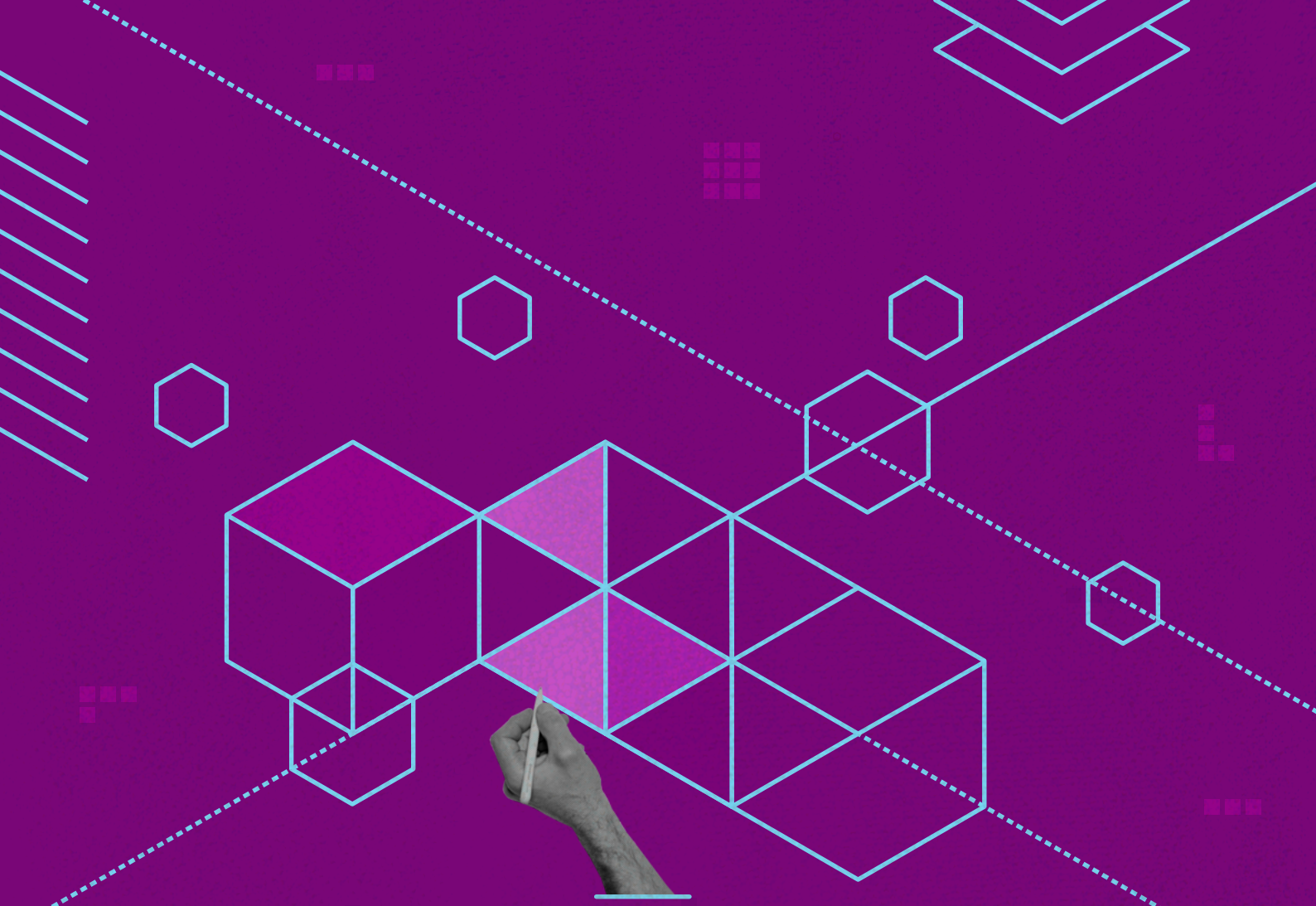
More broadly, platforms like AI Studio demonstrate how operational sandboxes offered by multinational technology companies can accelerate access to AI capabilities while also shaping how users experiment with, evaluate, and ultimately adopt AI within specific technological ecosystems.

[73] Wake Forest University (2025). Google AIStudio: your sandbox for AI experimentation with Google AI models, Wake Forest University.

Deploying AI is not only a technical upgrade but also a governance and organizational challenge, which requires new approaches to experimentation, oversight, and capability-building. Boards of Directors play a defining role in shaping how companies navigate the opportunities and risks of AI. As the bodies ultimately responsible for strategic direction and oversight, they are not only asked to approve AI investments, but to guide how these technologies are adopted, governed, and aligned with long-term organizational values. Yet, as AI adoption accelerates, gaps in board-level readiness are becoming visible.[74] AI sandboxes can offer a practical pathway for boards to fulfill their responsibilities and strengthen long-term resilience. They create controlled environments for experimentation, allowing organizations to test AI systems under real-world conditions while embedding safeguards, oversight mechanisms,[75] and cross-functional collaboration. For boards, this "test-and-learn" approach provides greater visibility into how AI systems perform, where risks materialize, and how governance frameworks hold up in practice. Importantly, sandboxes shift compliance from a reactive exercise to a proactive governance tool which enables boards to guide responsible innovation, build institutional capacity, and make more informed strategic decisions in a rapidly evolving technological landscape.

[74] Baig, A., Dave, A., Huber, C., and Vuppala, H. (2025). Elevating board governance through AI posture and archetypes. McKinsey & Company.

[75] Baig, A., Dave, A., Huber, C., and Vuppala, H. (2025). Elevating board governance through AI posture and archetypes. McKinsey & Company.



AI Sandbox Design: Challenges, opportunities and recommendations for business engagement

Quotes from consulted stakeholders

“The most useful sandboxes create richer environments for experimentation. Not because regulators need to solve the problem for startups, but because they can create better conditions for startups to solve problems properly.”

“The stakeholder approach is not just a design choice, it is what allows us to move from theory to practice and also to help ensure that what we develop is credible, it's practical, and ultimately scalable.”

“AI sandboxes often go deeper into models than traditional sandboxes. That enables serious work on things like fairness and explainability, but it also raises questions about intellectual property.”

"The regulator needs to play a role of helping to guide the company to understand what societal expectations are on these slightly more nebulous concepts. So that they can be translated into practical points that the company can operationalize.”

“What we have learned so far is that figuring out what to test is actually one of the biggest gaps today, and no single company has the answers. That's why we need collaboration across different groups."

Since most AI sandboxes are currently regulatory, this chapter presents five typical barriers to private sector engagement in these types of sandboxes and recommendations about how they can be overcome. The purpose of this chapter is to help policymakers have a better understanding of the current limitations of AI regulatory and hybrid sandbox models and share examples of how others addressed these issues.

While AI sandboxes can provide significant value for companies, their design and implementation often determine whether meaningful private sector engagement occurs or not. Common challenges include overly narrow sandbox scopes that do not reflect the complexity of real-world AI systems, limited awareness or readiness among potential participants, uncertainty around governance arrangements and how data, results, and liabilities will be managed, limited opportunities for realistic testing, and unclear pathways for translating sandbox participation into measurable outcomes beyond the experimentation phase.

Addressing these challenges requires intentional sandbox design, transparent communication, and mechanisms that ensure experimentation generates value for both participating companies, regulatory learning and the broader innovation ecosystem.

Narrow and limited AI sandbox scopes

A recurring limitation of AI regulatory sandboxes is the tendency for regulators to define **overly narrow scopes**, often focused on a single use case, technology, regulatory question or perspective that does not reflect the reality of real-world deployment. While it is important to define clearly what the sandbox is and is not, regulatory sandbox initiatives are often developed in isolation by one single regulator, even though AI systems and their impacts cut across regulatory and sectoral boundaries. While this can make the sandbox itself more manageable, it risks limiting the learning potential and reducing the relevance of outcomes beyond the immediate context. It can also limit private sector interest in setting aside significant resources to engage.

Design comprehensive sandbox scopes

Designing regulatory sandboxes through cross-regulatory collaborations can help capture interdependencies across sectors, better reflect real-world complexity and make them more useful for companies navigating cross-cutting regulatory regimes. What is more, while complex, developing mechanisms for cross-border recognition, or at least alignment in evaluation approaches and standards, can help extend the value of sandbox experimentation and reduce duplication of effort.

Box 9. Cross-regulatory coordination: the case of the Global AI Assurance Sandbox

Moving towards more integrated and cross-regulator sandbox ecosystems can be fostered by promoting coordination across multiple regulatory bodies, such as sector regulators and data protection authorities, and creating the conditions and incentives for collaboration. For example, the Global AI Assurance Sandbox developed by the Infocomm Media Development Authority (IMDA) in Singapore and the AI Verify Foundation provides a testing ground for builders or deployers of generative AI applications to have their systems assessed by specialist technical testers.[76] The sandbox is also open to sector regulators seeking to develop and refine AI governance or testing guidelines. Insights generated from sandbox testing feed directly into policy guidance and standards development,[77] illustrating the dual operational-regulatory function of hybrid models.

Box 10. Cross-border collaboration: the case of UK-Singapore AI-in-Finance Partnership

UK-Singapore AI-in-Finance Partnership is a strategic collaboration between the Monetary Authority of Singapore and the UK Financial Conduct Authority that enables safe and responsible AI innovation across both financial markets. The partnership facilitates joint testing of AI solutions, regulatory insight sharing, and cross-border knowledge exchange between two leading financial centres. By building on established programmes—MAS PathFin.ai and FCA AI Spotlight—the initiative strengthens AI collaboration and enables participants to scale best-in-class AI innovations more effectively across Singapore and the UK markets. Benefits for participants includes access to joint testing environments and regulatory sandboxes across both jurisdictions.[78]

Low levels of sandbox knowledge, readiness and access

Support the wider innovation ecosystem

Public officials can often report challenges in identifying appropriate and diverse regulatory sandbox applicants. Some of these challenges can be addressed early on before developing a sandbox initiative by strengthening the broader innovation ecosystem. Complementary investments in communications and outreach, capacity building, and partnerships with innovation hubs, technical universities and start-up incubators, can help develop a more diverse and capable pipeline of private sector participants.

[76] AI Verify Foundation(2025), Global AI Assurance Sandbox.

[77] IMDA (2025), Singapore launches new tools to help businesses protect data and deploy AI in a trusted ecosystem, IMDA.

[78] PathFin.ai (2026), PathFin.ai Programme and the UK-SG AI in Finance Partnership.

Box 11. Ecosystem coordination and SME engagement: the role of MRANTI in Malaysia's AI Sandbox

A key lesson from Malaysia's National Technology and Innovation Sandbox (NTIS)[79] is the importance of embedding AI sandboxes within broader innovation ecosystems rather than treating them as isolated instruments. In Malaysia, the sandbox is coordinated by the Malaysian Research Accelerator for Technology and Innovation (MRANTI), a national innovation accelerator with connections to startups, SMEs, universities, investors, and government agencies.

This positioning has enabled MRANTI to play a role beyond that of a traditional sandbox administrator. Acting as a trusted intermediary and ecosystem convener, MRANTI helps startups navigate fragmented regulatory processes, connects innovators with technical experts and investors, and facilitates collaboration across ministries, regulators, academia, and industry partners. This has been particularly important in supporting SMEs and early-stage AI startups that may lack the internal capacity, networks, or regulatory expertise to engage directly with government processes.

Importantly, MRANTI's broader innovation ecosystem functions also strengthen the sandbox pipeline itself. Through its existing relationships with local entrepreneurs, accelerators, universities, and innovation hubs, MRANTI is able to identify and support a more diverse pool of participants, including companies that may not traditionally engage in regulatory initiatives. The sandbox is therefore not only a governance mechanism, but also part of a wider national strategy to cultivate AI entrepreneurship, talent, and infrastructure.

Malaysia's experience highlights how selecting sandbox hosts with strong ecosystem ties and trusted relationships with innovators can help address a common challenge for regulators: identifying diverse and high-quality sandbox applicants while ensuring sustained private sector engagement.

Offer tiered innovation support for diverse ecosystem players

Many regulatory sandbox models implicitly assume that firms already have a clearly defined use case, sufficient product maturity, and the internal capacity to engage with regulatory processes. In practice, this can exclude early-stage startups, SMEs, or first-time AI adopters. Addressing this requires rethinking readiness not as a fixed threshold, but as a continuum. Offering not only regulatory sandboxes but **tiered innovation support**, such as advisory pathways, regulatory clinics, tech sprints or structured onboarding phases, can create more accessible entry points to the sandbox itself.[80]

[79] Government of Malaysia Ministry of Science, Technology and Innovation (2024), Malaysia's National Technology & Innovation Sandbox.

[80] Financial Conduct Authority (2022), Innovation Pathways, Financial Conduct Authority.

Design transparent and accessible participation pathways

Participation in regulatory sandboxes often requires significant time and resources, making a clear and credible value proposition essential from the outset. Clearly communicating expectations around product maturity, governance safeguards, and testing objectives in the call for applications helps prospective participants organizations assess their eligibility and prepare effectively. Lowering barriers to entry through simplified application processes, risk-based participation models, and if resources permit, funded cohorts can play a critical role.

Box 12. Funding participants: the cases of Singapore PETs sandbox and the European Digital Sandbox programme

Some sandbox initiatives provide direct financial and ecosystem support to participants, helping lower the costs and barriers associated with experimentation. For example, the Singapore PET Sandbox offered co-funding for pilot projects.[81] Grant support was provided (up to 50%) for eligible cost items during the project. Examples of cost items include manpower, professional services and hardware/software required for the 6 months project period.[82] This type of financial support makes it more attractive for private sector companies to participate.

Similarly, the European Digital Sandbox programme led by EIT Health[83] provided direct funding and matchmaking support to startups seeking access to sensitive health datasets, biobanks, and research partners across Europe. In 2020, six startups collectively received 180,000 EUR to support data access and experimentation activities related to healthcare innovation, diagnostics, and AI-enabled medical technologies.[84]

Uncertainty around governance, data use and sandbox outcomes

Uncertainty around intellectual property, confidentiality, data access, security, and liability can create friction and deter private sector participation, particularly in environments where sensitive data and proprietary technologies are involved. Without deliberate design, gaps or overlaps in accountability may emerge, particularly at the interaction points between actors.

[81] IMDA and PDPC (2022), Invitation to Participate in Privacy Enhancing Technology Sandbox "Pet Sandbox," IMDA.

[82] IMDA and PDPC (2022), Invitation to Participate in Privacy Enhancing Technology Sandbox "Pet Sandbox," IMDA.

[83] EIT (2020), The Digital Sandbox Accelerator.

[84] EIT Health (2020), Digital Sandbox helps six start-ups access key data.

Establish clear governance arrangements

Clear governance arrangements and well-defined terms help create the conditions for effective collaboration during execution. Furthermore, designing use cases that explicitly test these interaction points, such as between data and models, or models and deployment, can help surface how risks materialize in practice and support more realistic, system-level learning. These insights can then be used to inform more coherent and context-sensitive governance approaches beyond the sandbox itself.

Clarify legal responsibilities and terms of engagement

Closely related is uncertainty around the legal and regulatory status of sandbox participation. When expectations, protections, or consequences of testing are not clearly defined, companies may find themselves operating in a legal grey area. Clarifying liability frameworks, defining the boundaries of good-faith experimentation, and ensuring that participants understand how sandbox outcomes will be treated from a regulatory perspective are essential to building trust and enabling meaningful engagement.

Ensure transparent participation processes and communicate expectations early

Addressing and clearly communicating governance structures early in the sandbox process is important to manage expectations. At the same time, when participation is limited to a small group of companies, particularly without clear communication of selection criteria, there is a risk of perceived bias or regulatory capture, which can discourage broader engagement. Clearly articulating expectations around readiness, sectoral focus, and selection processes, as well as providing structured feedback to non-selected applicants, can help build trust and maintain ecosystem participation.

Lack of real-world testing abilities

Promising examples of hybrid AI sandboxes are emerging across various domains from fintech, Gen AI among others. However, constraints related to data access, rigid oversight structures, or lengthy review processes can restrict the extent to which technologies are tested in realistic and in fact “real world” conditions.

Enable safe and meaningful real-world testing

Strengthening the conditions for safe, supervised real-world testing is critical when preparing the execution of a sandbox advertised as such. This can include collaborating with multiple actors in sandbox execution, enabling access to representative datasets, establishing clear liability protections, and embedding experimentation within actual product development cycles rather than treating it as a one-off or purely exploratory exercise. For example, in hybrid sandbox models, data alone can sometimes not be enough for start-ups. Sandbox value often increases for start-ups when it is combined with compute, expert input, and realistic context around how the experimentation and product development happens. Providing sandbox mentors, facilitating industry communities and offering research advisors can help support a testing environment for start-ups that reflects how a business operates.

Box 13. Real-world testing: the case of AI Airlock

The UK's Medicines and Healthcare products Regulatory Agency (MHRA)'s AI Airlock Sandbox illustrates how sandboxes can enable safe and supervised real-world testing of AI systems, particularly in high-risk sectors such as healthcare. Developed as the UK's first regulatory sandbox for AI as a Medical Device (AIaMD), the program was designed to proactively address regulatory challenges faced by innovators and generate practical evidence on how AI systems perform in real operational contexts.

A defining feature of the AI Airlock is its **three-layer testing environments**, which progressively increase real-world testing while maintaining crucial safeguards. The three airlock environments include:

1. **Simulation airlock:** a workshop- or roundtable-based testing environment designed to explore specific regulatory questions through structured discussions and scenario-based exercises;

2. **Virtual airlock:** a "testbed" environment where AI models are tested using synthetic or real-world (retrospective) data. It enables developers to assess model performance, behavior, and reliability in research scenarios, generating technical evidence prior to deployment, and

3. **Real-world environment:** a controlled deployment of AI systems in clinical settings (e.g. National Health Service - NHS hospitals or with the intended user) under continuous oversight to observe their performance within the product's intended purpose workflows, while ensuring no impact on patient care.

This staged approach allows innovators and regulators to observe how AI systems behave within actual workflows, decision-making processes, and user interactions.

Concrete sandbox use cases highlight the value of this model. For example, OncoFlow tested its AI system for personalized cancer treatment planning using anonymized clinical data in simulated multidisciplinary team settings, enabling validation of both technical performance and clinical usability. In another case, within Newton's Tree's FAMOS platform, real-world testing helped identify patterns of over-reliance on AI outputs (automation bias) among users, an issue that may not have emerged in earlier testing phases but has direct implications for patient safety.[85]

[85] Medicines & Healthcare products Regulatory Agency (MHRA) (2025). AI Airlock Sandbox Pilot Programme Report, MHRA.

These experiences demonstrate that real-world testing can surface critical risks such as model drift, unreliable outputs, and human-AI interaction challenges, while also generating evidence on explainability, safety, and system integration. At the same time, the AI Airlock underscores that such testing requires careful design: strong oversight, access to representative data, and clear boundaries (e.g. distinguishing sandbox testing from formal clinical trials).[86]

Overall, as explained by the AI Airlock's report,[87] sandboxes are not clinical investigations, but structured environments for learning how AI performs in practice and what regulatory safeguards are needed for responsible deployment.[88] By embedding experimentation within real operational contexts, they are enabling both innovators and regulators to better understand how AI systems perform in practice and to develop more effective frameworks for their safe and responsible use.

Uncertainty of measurable impact

Since sandbox participation often demands sustained engagement from a company, including a dedicated team, recurring check-ins and the allocation of technical and legal resources, it is important that there are clear incentives and measurable impact for participants. Access to high-quality data, tailored regulatory guidance, and, where possible, fast-track approvals can help justify participation.

A persistent question for companies is often what happens after the sandbox ends. Solutions developed within sandboxes often struggle to transition into real-world deployment, particularly when moving across jurisdictions or regulatory regimes. Informal guidance or assurances provided during the sandbox do not always translate into formal approvals, and the cost structure for participants can shift significantly, from innovation and experimentation during the sandbox to operational, legal, and compliance requirements post-sandbox.

Share sandbox learnings, case studies and outcomes more broadly

Ensuring continuity beyond the sandbox also depends on how effectively outcomes are captured, evaluated, and communicated in ways that respect confidentiality and privacy. In practice, many sandbox initiatives do not systematically publish their findings, impacts, or lessons learned, limiting opportunities for broader ecosystem learning and reducing transparency around what approaches were effective, for whom, and under what conditions.

[86] Medicines & Healthcare products Regulatory Agency (MHRA) (2025). AI Airlock Sandbox Pilot Programme Report, MHRA.

[87] Medicines & Healthcare products Regulatory Agency (MHRA) (2025). AI Airlock Sandbox Pilot Programme Report, MHRA.

[88] Medicines & Healthcare products Regulatory Agency (MHRA) (2025). AI Airlock Sandbox Pilot Programme Report, MHRA.

Sharing anonymized sandbox learnings, case studies, and outcomes more broadly can further extend the measurable value of the sandbox beyond direct participants and support collective learning across the market. Partnerships with universities to assist with reporting and manage knowledge can also strengthen transparency, analytical depth, and knowledge exchange.

Box 14. Sandbox communication tools: the case of Norway Sandbox podcast and other outreach activities

An example of an innovative communications strategy for a sandbox is Norway's Data Protection Authorities Podcast: Personvernpodden. The podcast includes episodes within different series including one on their own sandbox bringing together sandbox participants and regulators to discuss the sandbox process and findings. This offers an approachable way for interested people to learn about the sandbox and share its wider insights.[89]

However, Norwegian Data Protection Authority communication strategy extended far beyond podcasts. The authority developed a broad range of externally directed activities aimed at disseminating lessons learned, increasing public awareness, and fostering broader discussions on responsible AI and data protection.[90] It created a dedicated sandbox section on its website containing application information, news, guidance materials, reports, and English-language resources to support international dissemination. Final reports were systematically produced for completed projects, helping translate sandbox experiences into publicly accessible regulatory and practical knowledge. Communication efforts also included newsletters, webinars, seminars, public events, opinion articles, editorial coverage, blog posts, and collaborations with external organizations such as Digital Norway to develop educational materials on personal data processing and AI governance.

Furthermore, Datatilsynet used the sandbox as a mechanism for broader regulatory learning and public guidance. In 2023, for example, it published a transparency report based on lessons derived from sandbox projects, including practical recommendations and checklists regarding transparency obligations in AI systems. According to the authority itself, this marked a shift from an initial phase focused on building expertise and project experience toward a broader strategy of making accumulated knowledge available to external stakeholders. The sandbox additionally served as a platform for inter-authority coordination and international engagement, including exchanges with foreign regulators and participation in European sandbox networks alongside authorities such as the UK's Information Commissioner's Office and France's Commission nationale de l'informatique et des libertés.

[89] Datatilsynet (n.d), The Privacy Podcast, Norwegian Data Protection Authority.

[90] Datitilsynet (2023). Evaluation of the Norwegian Data Protection Authority's Regulatory Sandbox for Artificial Intelligence. pp. 21-22.

Produce clear, structured outputs, such as toolkits, policy recommendations, testing methodologies, or implementation frameworks

Another important consideration is how sandbox learnings are translated into actionable outputs. Producing clear, structured outputs, such as toolkits, policy recommendations, testing methodologies, or implementation frameworks, can help bridge the gap between experimentation and real-world adoption. Sharing these insights more broadly, while respecting confidentiality constraints, highlights the actionable results of the sandbox, allows other actors in the ecosystem to benefit from the sandbox's findings and ultimately supports more consistent and evidence-based approaches to AI governance.

Box 15. Sandbox reporting: the Canton de Zurich AI Sandbox

A feature that stands out of the Canton of Zurich's AI sandbox is the quality, structure, and usability of its reporting. Rather than limiting outputs to descriptive accounts of pilot projects, each report systematically translates experimentation into actionable insights and both regulatory and technical recommendations for policymakers and innovators. Throughout the sandbox phases – spanning AI applications in public administration, healthcare, infrastructure, autonomous systems – reports consistently include clear conclusions, forward-looking outlooks, and concrete recommendations, ensuring that lessons learned are explicitly captured and can inform regulatory development, market adoption, and future sandbox iterations.[91]

Equally important is the sandbox's commitment to accessibility and knowledge dissemination.[92] Various use case reports are complemented by short explanatory videos, which ground the findings in concrete visuals from the sandbox testing. This makes complex regulatory and technical insights understandable beyond expert audiences. This combination of analytical depth reporting and user-friendly communication formats positions Zurich's sandbox as a leading example of how reporting can bridge the gap between experimentation and real-world policy impact.

Create clear post-sandbox pathways and define intended outcomes

Addressing uncertainty of sandbox impact also requires designing sandboxes with clear post-sandbox pathways from the outset, including mechanisms for regulatory follow-through, structured support for scaling, and clarity on how sandbox outcomes will be recognized or treated beyond the testing environment. The regulatory sandbox launched by the Agência Nacional de Proteção de Dados (ANPD), Brazil's Data Protection Authority, provides a clear example of a sandbox explicitly designed to inform regulatory interpretation and future guidance (see Box 16).

[91] Kanton Zürich (n.d.) Innovation Sandbox for AI. Phase II: 2024-2026.

[92] Innovation Zurich - YouTube Channel.

Box 16. Intentional design for regulatory learning: the case of Brazil's ANPD Sandbox

The regulatory sandbox launched by the Agência Nacional de Proteção de Dados (ANPD), Brazil's Data Protection Authority, provides a clear example of a sandbox explicitly designed to inform regulatory interpretation and future guidance. The initiative was first announced through a public call for contributions in 2023,[93] aimed at exploring the intersection between artificial intelligence systems and data protection rules under the Brazilian data protection framework, the *Lei Geral de Proteção de Dados* (LGPD).[94] One of the central goals identified by ANPD was the promotion of algorithmic transparency, particularly in systems based on machine learning paradigms, including generative AI. Algorithmic transparency in this context refers to making the functioning of AI systems and their decision-making processes understandable and explainable, enabling the identification of potential biases or discriminatory practices while fostering accountability and trust among users and stakeholders.

The sandbox directly addresses legal uncertainties related to Article 20 of the LGPD, which establishes the right of individuals to request the review of decisions made solely on the basis of automated processing that significantly affect their rights or produce legal effects. This provision is particularly relevant for AI systems involved in decision-making processes such as credit scoring, hiring, or profiling for targeted advertising. Moreover, generative AI systems raise additional concerns, as they may generate inaccurate or misleading personal data about individuals. ANPD's sandbox is allowing the authority to better understand how the transparency and review requirements established in Article 20 - and specifically its §1º - should be interpreted and implemented in the context of emerging AI technologies.

The initiative also aims to support regulatory learning in light of ongoing legislative debates on AI governance in Brazil, where Bill nº 2338/2023, a.k.a. "AI Bill", includes provisions related to automated decision-making and transparency obligations. Through the sandbox, ANPD seeks to assess the legal compatibility and interoperability between the LGPD and future AI legislation. In 2025, the authority launched a call for sandbox participants, reiterating these learning and guidance objectives. Despite the fact that the sandbox does not provide financial resources or dedicated digital infrastructure to participants, the clarity of its regulatory learning goals generated significant interest. The call attracted 17 applicants, including international companies, and ultimately resulted in the selection of three pilot cases for participation in the sandbox program.[95]

[93] Ministry of Justice and Public Security (2023), ANPD's Call for Contributions to the regulatory sandbox for artificial intelligence and data protection in Brazil is now open, Government of Brazil.

[94] Agência Nacional de Proteção de Dados Brazil (2024) Lei Geral de Proteção de Dados (Brazilian Data Protection Law), Government of Brazil.

[95] Ministry of Justice and Public Security (2025), Following appeals, ANPD publishes final results of the Regulatory Sandbox project, Government of Brazil.

Importantly, the initiative also incorporated a structured onboarding phase. After the selection process, ANPD organized a "leveling" session with the selected participants to align expectations and ensure that companies clearly understood the sandbox's objectives, regulatory questions, and methodological approach. This onboarding stage was designed to facilitate dialogue between the regulator and participants and to ensure that the experimentation process would effectively generate insights relevant for regulatory guidance. In short, ANPD's sandbox illustrates how sandboxes designed primarily around regulatory learning and guidance - rather than direct financial incentives - can still attract strong participation from stakeholders seeking legal certainty in rapidly evolving technological domains.

The sandbox also benefits from technical support provided by the Center for Artificial Intelligence and Machine Learning (CIAAM) at the University of São Paulo (USP). The Center contributes scientific and technical expertise to the evaluation of AI systems, supporting the methodological aspects of the experimentation process and helping to identify technical issues relevant to regulatory analysis. This collaborative model combines regulatory oversight with independent academic expertise, strengthening the evidence-based approach adopted by ANPD while preserving the authority's decision-making autonomy.

Conclusion

As AI sandboxes grow and mature, business engagement will become an increasingly vital practice for ensuring sandboxes serve both innovators and the broader public interest. Sandboxes can help educate policymakers and businesses on the ways to approach technology and regulations in ways that are protective, responsible and innovation enabling.

However, as this report has demonstrated, **the value of AI sandboxes for businesses is neither uniform nor automatic**. It depends on how sandboxes are designed, the type of model adopted, and the characteristics and position of firms within the AI value chain. When effectively implemented, sandboxes can reduce uncertainty, lower the costs and risks of innovation, and accelerate learning and market readiness. At the same time, they offer businesses a structured environment to engage with regulators, build trust, and navigate complex governance landscapes.

Importantly, sandboxes are not only tools for firm-level experimentation. They are emerging as system-level mechanisms that connect AI technical development, regulatory oversight, and real-world deployment. By enabling testing across different layers of the AI value chain and fostering collaboration among interdependent actors, sandboxes could help clarify roles and responsibilities, surface risks earlier, and support more adaptive and evidence-based governance approaches.

Looking ahead, **the effectiveness of AI sandboxes will depend on the ability of both public and private actors to move beyond fragmented approaches and engage with sandboxes as shared infrastructures for learning and coordination**. For policymakers, this means designing sandboxes that are inclusive, transparent, and responsive to the realities of AI systems as interconnected socio-technical ecosystems.[96] For businesses, it means approaching sandbox engagement not only as a compliance or innovation exercise, but as a strategic opportunity to shape emerging standards, strengthen governance practices, and position themselves as trustworthy within AI markets.

There is also a need to move beyond isolated experimentation toward more standardized and interoperable approaches. The lack of alignment across sandboxes within and between countries limits their broader impact for broader regulatory learning and particularly for companies operating across jurisdictions. Developing common standards, shared definitions of good practices, as well as mechanisms for cross-border recognition of sandbox outcomes, can help scale learning and reduce duplication of effort.

[96] Leeds University Business School (s.f.) Socio-technical systems theory. University of Leeds.

Realizing this potential also requires broadening who sits at the table. AI sandboxes have largely been structured around business-to-government dynamics, but communities most affected by AI systems (e.g., civil society organizations, advocacy groups, researchers, and end users) bring perspectives that neither regulators nor industry can substitute. Future work should explore how sandboxes can be designed to meaningfully incorporate civil society as active participants, not merely as consultees or oppositional critiques,[97] ensuring that the evidence and standards they generate reflect a wider range of values, risks, and lived experiences.

This report is a first step in understanding the role the private sector plays in AI sandboxes supporting both the private and public sector as they design sandbox models and practices. The Datasphere Initiative plans to develop additional research and guidance for civil society and other stakeholders in sandbox design and engagement.

Ultimately, AI sandboxes provide a unique opportunity to bridge the gap between innovation and governance. Their long-term impact will lie in their ability to translate experimentation into better policies, more robust systems, and more responsible and trustworthy AI.

[97] Datasphere Initiative (2026), Sandboxes for DPI: Co-creating the blocks of digital trust, Datasphere Initiative.

Annexes

Annex I: Guidance for Business

AI Regulatory Sandbox Business Participation Checklist

Getting the most out of AI regulatory sandboxes

A practical guide for businesses considering participation in AI regulatory sandboxes.

This practical resource provides a checklist for companies considering whether to participate in AI regulatory sandboxes. It can be used as a conversation starter with your board, a practical guide for in-house policy teams or a sandbox introduction guide for a start-up or SME. This is your quick-reference guide for before, during and after participation in the sandbox.

Who is this for?

Boards • Executives • Legal & Compliance Teams
Product Teams • Start-ups • SMEs

What is an AI Sandbox?

A controlled learning environment in which AI systems, use cases, or related governance approaches are tested under defined conditions, timeframes, and safeguards, enabling iterative experimentation, evidence generation, and shared learning among multiple stakeholders to inform both innovation and governance.

What is an AI Regulatory Sandbox?

An AI sandbox centered on regulatory learning or compliance, designed to generate evidence that informs existing or future rules, policies, standards, and guidance as they relate to AI.

Why join an AI Regulatory Sandbox?

Regulatory validation	Enhanced business legitimacy	Reduced regulatory uncertainty	Reduced compliance risks
Controlled pre-deployment testing	Regulatory flexibility	Structured engagement with regulators	Visibility within the innovation ecosystem

How to use this checklist

- ✓ Assess whether an AI regulatory sandbox is right for your organization
- ✓ Prepare for participation in an AI regulatory sandbox
- ✓ Engage effectively with regulators
- ✓ Maximize commercial and regulatory value throughout the sandbox lifecycle

What is the typical process for participants of an AI Regulatory Sandbox?

1 AI sandbox selection and application

- Identify an AI sandbox that aligns with the organization's business needs
- Apply
- Application accepted

2 Process definition and organization resource alignment

- Sign NDA or other terms of engagement
- Attend a cohort onboarding session

3 Sandbox implementation

- Attend first meeting to identify key questions or testing areas of mutual interest to the organization and regulators and agree on testing plan
- Attend a series of workshops/meetings to conduct the testing plan

4 Learnings and recommendations

- Obtain exit report with regulatory guidance and details (this report is not for public consumption and can contain sensitive information)
- Regulatory authority publishes report with wider regulatory learnings and relevant guidance for the ecosystem

Typical duration between 3-6 months

How can I successfully leverage the opportunity?

Before participation

Assess your readiness and business alignment with sandbox testing objectives before applying.
Carefully review the sandbox's eligibility criteria and expectations, and evaluate your organization's business needs, use case, product maturity, team availability, governance capacity and financial viability for the duration of the project to determine fit. The closer the match between the sandbox's objectives and your company's development stage and testing needs, the greater the likelihood of a meaningful and productive experience.

Strengthen your capabilities in advance.
If justified, invest in building internal processes, responsible AI practices, and partnerships (e.g., with universities or innovation hubs) to improve your readiness for participation. Also ensure or prepare to have qualified personnel across multiple functions (technical, legal, and operational) who can actively participate in the sandbox testing process. Effective involvement demands continuous commitment, expertise, and the flexibility to adjust the product based on feedback gathered throughout the testing phase.

Engage proactively with sandbox hosts and seek explicit written assurances about data handling and IP.
Use application and participation processes to signal your needs, constraints, and context, helping regulators better understand how to design more accessible and effective sandboxes. Seek explicit written assurances about how your data, findings, and intellectual property will be handled, stored, and disclosed. Assess the sandbox's reporting obligations early and do not assume confidentiality is implied, ensure it is clearly defined in the governance framework. Align on scope of publicly released reports and whether participation will be anonymized or attributed.

Define your learning goals, innovation priorities, and internal and external metrics before committing.
Priorities can vary from understanding regulatory expectations and testing the ethical or legal robustness of a technology, to exploring potential applications of AI under new governance frameworks, market access, data access, or boosting visibility and reputation. This is particularly useful in highly regulated industries like finance or healthcare. Defining these objectives and their measurements, both internally and externally early ensures participation is strategic and aligned with your innovation roadmap.

Frame your objectives within your role in the AI value chain.
Firms operating at different layers - such as data provider, infrastructure, model development, or application deployment - face distinct technical challenges and regulatory expectations. Clarifying your position helps define more targeted sandbox objectives and surface dependencies and shared responsibilities across partners, suppliers, and clients.

During participation

Maintain a clear internal protocol for what information is shared within the sandbox and under what conditions.
Define internally what information about your products and services could be disclosed to the sandbox host, or publicly to third parties. Safeguarding competitive advantages and proprietary information requires active management throughout the sandbox process. Engage proactively with the sandbox host to ensure continued alignment on the purpose and scope of public-facing outputs including reports, press releases, and case studies.

Approach sandbox participation as a trust-building exercise in both directions.
Companies that engage openly and in good faith are better positioned to shape the regulatory dialogue, build credibility with policymakers, and contribute to governance frameworks that reflect their operational realities.

Assess and monitor the potential financial and associated costs of participation on an ongoing basis.
If resource strain becomes significant, engage proactively with the sandbox host to explore whether simplified reporting, phased commitments, or other adjustments are possible.

After participation

At the close of the sandbox, conduct a structured internal evaluation of the extent to which your learning goals and innovation priorities were met.
Assess the regulatory clarity gained, feedback received, relationships built with regulators and co-participants, and any tangible outputs such as formal opinions, exit reports, or guidance notes.

Use sandbox outcomes to inform your broader governance and innovation roadmap.
Insights gained during participation, whether about regulatory expectations, technical risks, or ecosystem dynamics, should feed directly into product development, compliance strategy, and future regulatory engagement decisions.

If the sandbox has not produced the regulatory clarity or formal outputs expected, engage with the sandbox host and relevant regulators.
Ask for clearer follow-up mechanisms — such as presumption of conformity notes, formal regulatory opinions, or documented guidance — that translate experimentation into actionable compliance benefits.

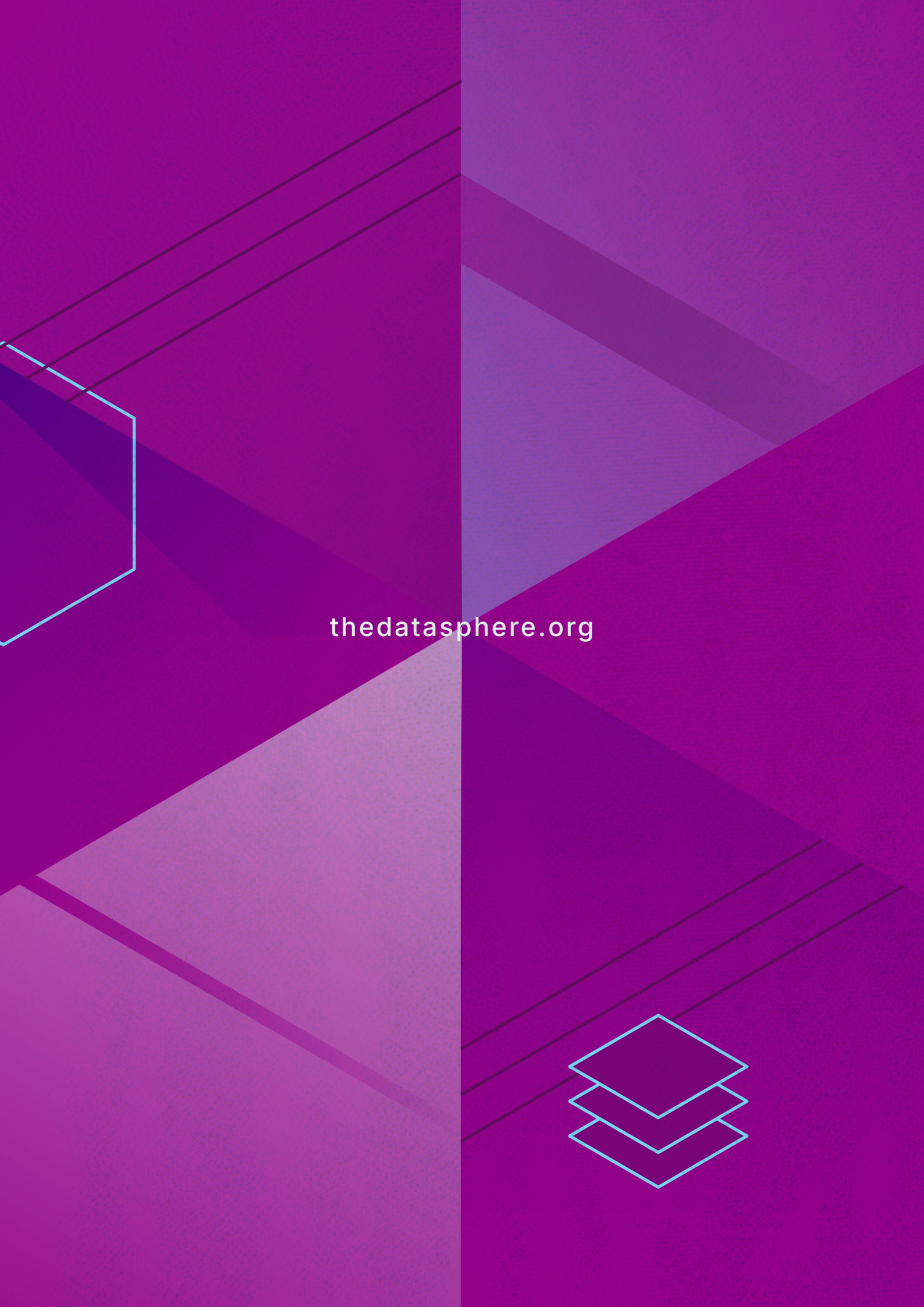
Consider sharing learnings or participating in sandbox-published case studies where appropriate.
Contributing to public knowledge builds credibility, strengthens your position in regulatory dialogues, and helps shape the standards and frameworks that will govern your market.

Annex II: Thematic Indexes

Index by Sandbox (Alphabetical Order)

- **AI Airlock Sandbox (UK MHRA)**
  - Found in: Box 14 (Theme: Real-world testing)
- **Global AI Assurance Sandbox (Singapore)**
  - Found in: Box 3 (Theme: Businesses as technical providers in hybrid sandboxes) & Box 11 (Theme: Cross-regulatory coordination)
- **Brazil's ANPD Sandbox**
  - Found in: Box 13 (Theme: Intentional design for regulatory learning)
- **Canton of Zurich AI Innovation Sandbox**
  - Found in: Box 18 (Theme: Sandbox reporting)
- **Central Bank of Ireland Innovation Sandbox Programme**
  - Found in: Box 17 (Theme: Fostering trust)
- **European Digital Sandbox programme**
  - Found in: Box 15 (Theme: Funding participants)
- **FCA Digital Sandbox (UK)**
  - Found in: Box 8 (Theme: Access to compute and data in a hybrid sandbox)
- **Google's AI Studio Sandbox**
  - Found in: Box 10 (Theme: Operational sandboxes offering a "try before you integrate")
- **Malaysia's National Technology and Innovation Sandbox (NTIS) / Malaysia's AI Sandbox**
  - Found in: Box 12 (Theme: Ecosystem coordination and SME engagement)
- **Norway Data Protection Authority's Regulatory Sandbox**
  - Found in: Box 6 (Theme: The value of regulatory sandboxes for SMEs) & Box 16 (Theme: Sandbox communication tools)
- **SandboxAQ**
  - Found in: Box 4 (Theme: Business as a host of an operational sandbox)
- **Singapore PET Sandbox**
  - Found in: Box 15 (Theme: Funding participants)
- **UK FCA Supercharged AI Sandbox**
  - Found in: Box 8 (Theme: Access to compute and data in a hybrid sandbox)
- **Unnamed hybrid sandbox initiatives (United Kingdom, Malaysia)**
  - Found in: Box 5 (Theme: The growing role of infrastructure providers in hybrid sandbox models)

Index by Box (Numerical Order)


thedatasphere.org