ASSOCHAM®
Ideate · Innovate · Impact

Shardul Amarchand Mangaldas
A DECADE YOUNG, A CENTURY STRONG

GOVERNANCE MECHANISMS TO PROMOTE OPEN SOURCE AI SYSTEMS:

AN INDUSTRY PLAYBOOK

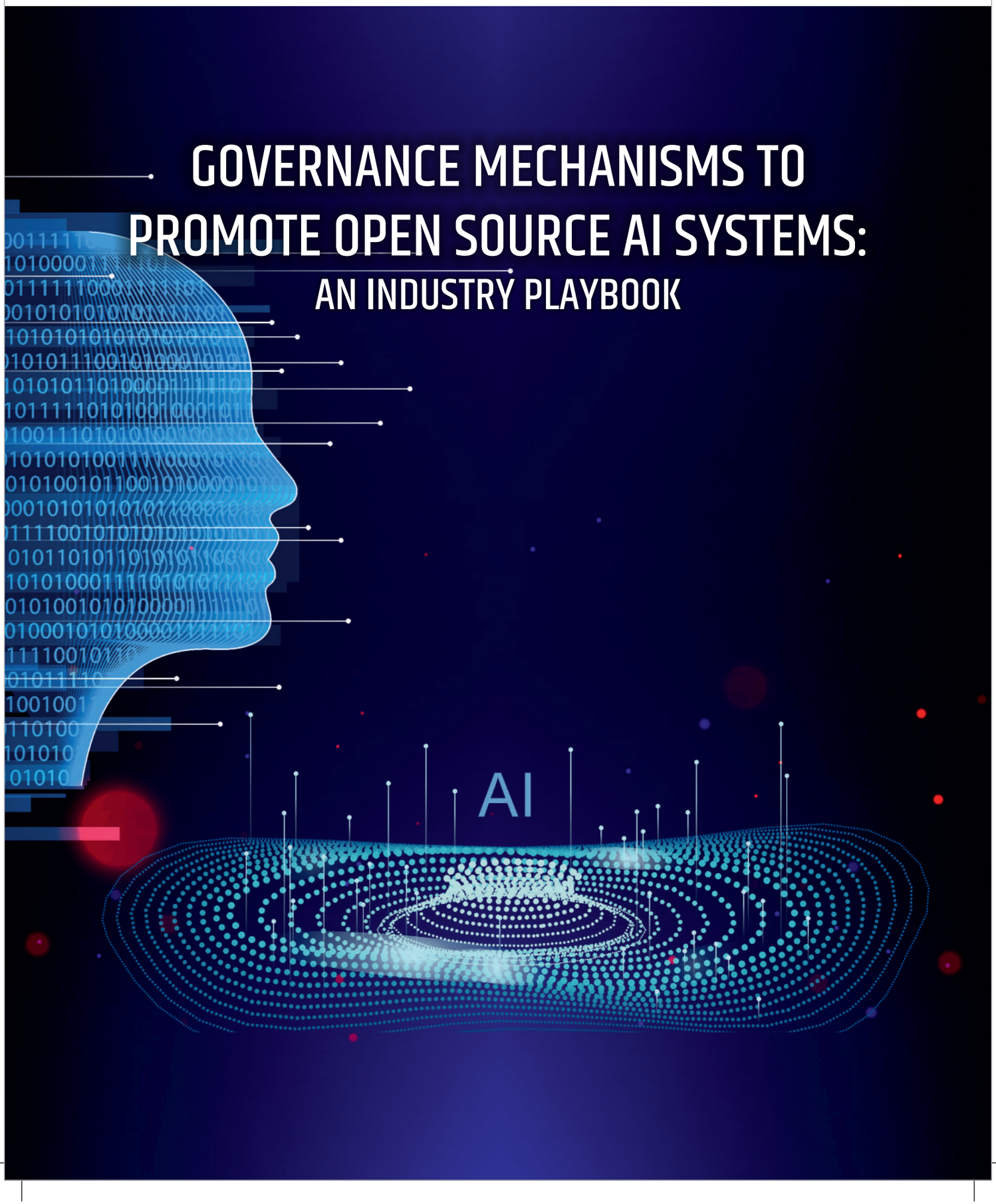


TABLE OF

CONTENTS

Foreword

Artificial Intelligence is undergoing a global transformation, driven significantly by the rise of open-source AI systems. Across nations, open-source AI is enabling faster innovation, greater transparency, and broader participation in the AI ecosystem. By encouraging shared development, reusable components, and open access to tools and model architectures, open-source AI is becoming a cornerstone for building trustworthy, accountable, and interoperable AI solutions. At the same time, the international community recognises the need for robust governance mechanisms to ensure safety, security, responsible data use, and ethical deployment.

As open source AI moves from the margins to the mainstream of innovation, the report offers a grounded view of the governance measures shaping its responsible adoption across sectors, and situates these developments within India's evolving AI landscape. Open source AI matters because it accelerates innovation, broadens participation, and reduces barriers to entry while reshaping the contours of risk around data governance, intellectual property and user safety. Getting this balance right is essential to building trust and competitiveness in India's digital economy.

The report recognises that "open" is not binary in AI. Instead, openness sits on a spectrum across layers such as code, data, model weights, training processes, and deployment infrastructure. The playbook sets out a clear framework for assessing degrees of openness through four criteria-role allocation, transparency, licensing, and risk management-so that stakeholders can make calibrated, context-specific choices rather than one-size-fits-all decisions.

The Ministry of Electronics and Information Technology (MeitY) has played an instrumental role in fostering responsible AI practices, supporting research and innovation, and shaping policy frameworks that encourage openness while safeguarding user trust. As India progresses toward the vision of Viksit Bharat, strong governance frameworks will be critical to ensuring that open-source AI systems are secure, ethical, and aligned with national priorities. ASSOCHAM has consistently worked to strengthen India's technology and innovation landscape. This report reflects our commitment to supporting MeitY and the Government of India in building a future-ready AI ecosystem.

The report also outlines practical governance models commonly used in the private sector and explains how each can be tailored for Indian use cases. For instance, licensing choices-permissive, copyleft, or responsible-use licences-and tiered commercial terms can be used to balance openness with safety while furthering commercial objectives.

I am confident that this report by ASSOCHAM and SAM will serve as a valuable resource for all stakeholders working towards strengthening India's leadership in responsible open-source AI.

Manish Singhal
Secretary General
ASSOCHAM

Message

The 9th ASSOCHAM AI Leadership Meet 2025 returns with renewed focus under the theme "AI: From Idea to Impact", reflecting our commitment to advancing actionable and scalable AI adoption across sectors.

Globally, AI is progressing at extraordinary speed, with open-source AI emerging as a key driver of innovation for impact at scale. By enabling developers, researchers, and enterprises to access, validate/analyze, and improve models collaboratively, open source is helping nations build more transparent, trustworthy, and inclusive AI ecosystems.

In India, the Ministry of Electronics and Information Technology (MeitY) continues to shape a strong policy and innovation environment through initiatives such as IndiaAI, the National Programme on AI, and the country's digital public infrastructure. These efforts underscore a national vision where openness, trust, safety, and innovation reinforce each other. Open-source AI aligns deeply with this vision, offering India a pathway to accelerate indigenous capabilities, support startups, and democratize access to advanced AI tools.

It is in this context that ASSOCHAM, in collaboration with Shardul Amarchand Mangaldas & Co., is releasing the Open Source AI Governance Report. The report provides a clear and practical framework for responsible and innovation-friendly open-source AI deployment, addressing issues such as safety, transparency, licensing, role allocation, and risk management. It is designed to help organisations navigate the rapidly evolving AI landscape with confidence and accountability.

This Leadership Meet also serves as a pre-summit engagement for the AI Impact Summit 2026, adding greater significance to the insights and outcomes we anticipate. The discussions held here will help shape a broader national and global dialogue on accelerating AI innovation for economic growth, societal benefit, and long-term technological leadership.

As Chair of the ASSOCHAM AI Taskforce, I extend my sincere appreciation to the teams at ASSOCHAM and Shardul Amarchand Mangaldas & Co. for developing this timely and impactful report. I am confident it will serve as a valuable resource for industry leaders, innovators, and policymakers as we work together to realise the vision of a Viksit Bharat 2047 powered by safe, transparent, and inclusive AI.

Sandip Patel
Chair, ASSOCHAM National Taskforce on
Artificial Intelligence

I Introduction

Open sourcing is critical for advancing the development of Artificial Intelligence ("AI") technologies as openness democratizes access to cutting-edge models and tools by making them available to individual developers, start-ups, and researchers. Especially in a developing economy like India, open source AI can help foster innovation by enabling developer communities to collectively scrutinize, build upon, and refine existing code, algorithms, and architectures. This can in turn lead to faster bug fixes and the creation of novel applications. Furthermore, open source promotes transparency and accountability, allowing for examination of a model's inner workings to detect and mitigate potential biases or ethical issues, ultimately fostering greater trust in AI systems.

Given the many benefits of open sourcing, this Playbook aims identify ways in which technology companies in India can benefit from putting in place governance measures to make open source AI more pervasive. To this end, Section II of this Playbook looks at the varied meanings of open source in the context of generative AI (**"GenAI"**) systems[1]. Based on this review, Section II suggests looking at open source as a spectrum rather than viewing it in binary terms. This is in line with the Organisation for Economic Cooperation and Development's (**"OECD"**)[2] approach to open source AI. In its paper on 'AI Openness', the OECD has recognised that openness in the context of AI exists on a spectrum and is not binary. This growing recognition of a spectrum of openness is also reflected in ongoing discussions and interpretations pertaining to the EU AI Act[3].

As this is a playbook concerned with the governance of open source AI, Section III looks at the most prevalent models for open source governance in the private sector and evaluates their openness across 4 key criteria- (i) role allocation, (iii) transparency, (iv) licensing, and (v) risk management. The 4 criteria help define the degrees of openness across different governance models. Section III highlights the relative merits of each of these governance models.

Finally, Section IV discusses the competing considerations in choosing a particular model of governance for AI projects.

---

[1] *Unless expressly stated otherwise, all references in this Report to 'AI systems' or 'AI models' refer specifically to generative artificial intelligence does not include other non-generative AI techniques.*

[2] *The OECD working paper on AI openness explicitly articulates a "spectrum of openness" for AI models, see <https://www.oecd.org/en/publications/ai-openness_02f73362-en.html>.*

[3] *The European Commission established an AI forum for cooperation with the open source community, "with a view to identify and develop best practices for the safe development and use of open source AI models and systems." While the binary open source exemptions under the EU AI Act have not been fundamentally redefined, this AI forum is operational and provides a space for discussion of graduated or nuanced approaches to open source AI governance, rather than strict binary classification, see <https://artificialintelligenceact.eu/responsibilities-of-european-commission-ai-office/>.*

II Defining Open Source AI

Defining “open source” in the context of GenAI is challenging because openness is not a binary distinction between open and closed systems. Rather, openness in the context of GenAI is better understood as a spectrum. Unlike traditional software, where open source is largely tied to licensing and access to source code, GenAI systems involve multiple layers such as training data, models, weights, training processes and deployment infrastructure. GenAI systems may have different levels of openness across these layers making it difficult to settle on a single definition.

For instance, some GenAI models are released with publicly accessible code and weights but restrict access to training data, while others release only the code or allow access under restrictive licenses[4]. Such distinctions in both the design and deployment of GenAI systems makes it difficult to establish a unified definition of open source AI. The task of defining open source AI is further complicated by ongoing debates regarding legal and ethical implications over what constitutes openness in GenAI systems[5]. Given the challenges in establishing a definition of open source AI, there is growing recognition that openness should not be treated as a 'yes-or-no' condition.[6]

Relying on a spectrum of openness to identify different types of open source AI models would mean examining the levels of openness accorded to the inner workings of GenAI models. This could be based on whether certain components of the GenAI model are made publicly available (e.g., documentation, weighting factors, information on the model architecture or usage, etc.). Considering the differences between GenAI and conventional software, there is experimentation with respect to different degrees of openness in the course of product development. Therefore, any approach that views openness as composite and graded will be is a reflection of operational realities, as opposed to a simple open or closed binary.

[4] *See for a discussion on different licensing strategies in AI systems, <https://opensource.org/blog/state-of-the-source-at-ato-2025-state-of-the-open-ai>. For a discussion on Dual Use Foundation Models, see <https://www.ntia.gov/programs-and-initiatives/artificial-intelligence/open-model-weights-report/background>*

[5] *Yaniv Benhamou, "Open Source AI - definition and selected legal challenges", available at <https://legalblogs.wolterskluwer.com/copyright-blog/open source-ai-definition-and-selected-legal-challenges/> and Edd Gent, "The tech industry can't agree on what open source AI means. That's a problem.", available at <https://www.technologyreview.com/2024/03/25/1090111/tech-industry-open source-ai-definition-problem/>.*

[6] *Hugging Face for instance makes the case for a more nuanced understanding on what constitutes openness across 6 criteria. See, Irene Solaiman, "The Gradient of Generative AI Release: Methods and Considerations" (Preprint, under review), available at <https://arxiv.org/pdf/2302.04844>.*

Figure1: Criteria for Openness

Accordingly, for the purposes of this Playbook, we have taken a broader view of the AI ecosystem and outlined the following 4 criteria to classify GenAI systems:

a. Role Allocation

The role of different actors in a GenAI system may vary and overlap across GenAI systems. Actors in the open source AI value chain – such as developers, deployers, and users – cannot be easily assigned clear-cut or static roles because their responsibilities and interactions are complex and overlapping. Open source AI systems involve dynamic collaborations where actors may contribute to the development, deployment, risk management, and governance at various points and in different capacities. Thus, the same individual or entity may take on multiple roles depending on the context. For example, a developer who contributes code may also serve as a deployer of downstream systems.[7] Similarly, an external contributor might engage in ethical oversight while also contributing to development of the training model. In centralised forms of governance, roles can be clearcut, with most functions managed internally by the governing entity. In more decentralised models of governance, roles are distributed with multistakeholder boards, working groups, sponsors, and contributors managing the project.

Role fluidity across actors in an AI system is evident in the Indian AI ecosystem where development, deployment and evaluation cannot be segregated into different organisational entities. The India AI Governance Guidelines[8] ("AI Governance Guidelines") acknowledge that this reality by noting that actors in the AI value chain operate at different layers and perform dynamic functions through "complex inter-personal relationships".

[7] *For a discussion on defining roles in complex AI value chains, see Philipp Hacker, Ramayya Krishnan and Marco Mauer, "Global AI Governance-Part 1: Decoding Developers and Deployers", Oxford Business Law Blog, available at <https://blogs.law.ox.ac.uk/oblb/blog-post/2024/12/global-ai-governance-part-1-decoding-developers-and-deployers>.*

[8] *India AI Governance Guidelines, Ministry of Electronics and Information technology, Government of India, see https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc2025115685601.pdf.*

b. Transparency

Transparency is a foundational characteristic of open source GenAI systems. Transparency allows stakeholders and users to move beyond treating AI as a "black box" and enable them to verify if a GenAI system adheres to its intended purpose without causing unintended harm. Transparency also helps foster collective accountability and allows stakeholders to validate the system's security, reliability, and ethical standards. However, transparency in a GenAI system may also lead to risks because allowing access to a wider set of stakeholders could make a GenAI system vulnerable to external threats.[9] Therefore, GenAI systems adopt different strategies to transparency while balancing openness against the need to protect and GenAI system against external threats *(see Risk Management at para (d)* below).

A GenAI system focussed on minimising external threats may choose to “open” its base code while keeping information related to its decision-making processes and risk management “closed”. On the other hand, a more open system may choose to disclose its models, datasets and codes with rigorous documentation. Such systems may pursue a more decentralised risk management strategy through expert committees made up of a wide range of external stakeholders.

c. Licensing

Licensing arrangements define the legal framework that governs how a GenAI system's code, weights, and its training data can be used, modified, and shared. Licensing choices are a primary determinant of how “open” a GenAI system or governance mechanism is in practice, because they set the conditions under which participation, reuse, and downstream decision-making can occur. In effect, the license calibrates permeability between open and closed layers, shaping whether governance remains centralised or is shared with the community. Permissive licenses (like MIT or Apache 2.0) are used even in proprietary products.[10] Copyleft licenses (like the GPL) mandate that any derivative work must also be shared under the same open terms. Newer licenses, such as Responsible AI Licenses (RAIL), place ethical restrictions on use or prohibiting applications that could cause harm.[11] Licensing arrangements also play important gatekeeping functions in GenAI systems that are partially opened or partially closed. Tiered licensing for different end uses is an increasingly popular way of commercialising products while keeping some layers of a GenAI system open to community feedback.

---

[9] *National Telecommunications and Information Administration (NTIA), "Earned Trust through AI System Assurance", available at <https://www.ntia.gov/programs-and-initiatives/artificial-intelligence/open-model-weights-report/risks-benefits-of-dual-use-foundation-models-with-widely-available-model-weights/public-safety>.*

[10] *FOSSA, "Open Source Licenses 101: Apache License 2.0", available at <https://fossa.com/blog/open source-licenses-101-apache-license-2-0/>.*

[11] *For a discussion on different open source licenses for AI, see <https://cycode.com/blog/open-source-licenses-made-simple/>*

b. Risk Management

As discussed in para (b) above, while openness has many benefits, it can simultaneously increase exposure to external threats. For instance, the ability for more stakeholders to inspect and modify the code in a GenAI system can introduce security vulnerabilities and lead to the misuse of the training model[12].

Risk management strategies are weighed against considerations around liability. Governance models that adopt a more centralised structure establish internal risk management processes that are run almost entirely by the governing entity that controls the GenAI system. This is because the governing entity would likely bear primary liability for any harm or misuse of the GenAI system.

On the other hand, more decentralised GenAI systems may pursue strategies where the liability risk is also distributed across expert committees, core and external contributors. However, the allocation of risk management responsibilities with respect to the distribution of liability and accountability is generally determined by the contractual arrangements negotiated between stakeholders.

Based on the criteria outlined above, we discuss 4 kinds of governance models used in GenAI systems in Section III.

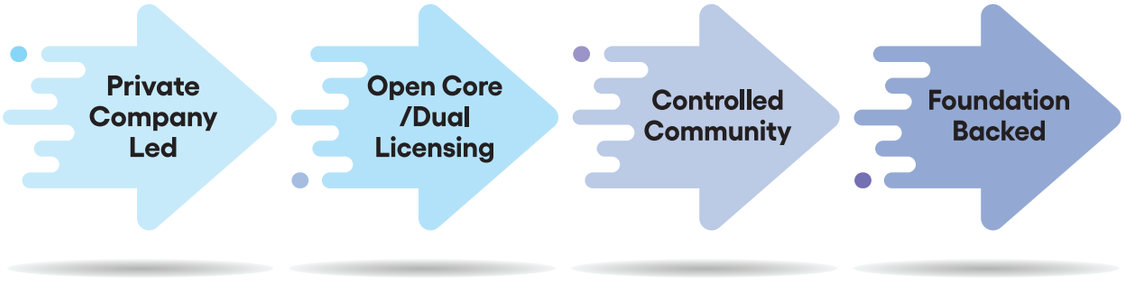
[12] *Supra, NTIA, note 9.*

III Open Source AI Governance Frameworks

Open source AI systems require robust governance frameworks to ensure responsible development, deployment, and oversight. The complexities of a GenAI system require clear, enforceable structures that balance openness with accountability, safety and ethical considerations. GenAI systems adopt a variety of governance frameworks that shape how decisions are made, who holds authority, and how contributors participate. While we acknowledge the diversity of these frameworks, the Playbook is limited to exploring different governance models used in the private sector.

This Playbook has examined 4 categories of open source AI Governance Frameworks. Each model of governance is defined by its own unique structure built to suit specific project outcomes. The 4 models have been classified based on how their governing bodies are constituted and which entities/individuals are empowered to make decisions. As we will see below, the governance design of each project is not merely a feature of a GenAI system. The overall governance of a project also dictates how open or closed each layer of the GenAI system is. Here, licensing functions as the practical gatekeeper of openness across models, operationalising governance choices by defining what can be accessed, adapted, and redistributed. As a result, similar governance architectures may have materially different degrees of openness depending on their licensing regimes. We discuss below the 4 types of AI governance models used in the private sector and also describe how they compare against the criteria for openness discussed in Section II.

Figure2: Models of Open Source AI Governance



a. Private Company Led Governance:

A private company retains centralised decision-making authority over an AI project, while releasing portions of it under an open source license. All crucial governance decisions ranging from feature roadmap to design choices and the timing of releases

are made internally by the corporate team. External contributors have little or no formal role in the project's governance.

(i) **Role Allocation:** Core development and architecture are overseen by in-house teams. External involvement, where permitted, is limited to non-critical contributions, such as bug fixes and minor features, while all significant project functions and accountability remain with the company.

(ii) **Transparency:** Public access is typically limited to the base code, with minimal disclosure regarding decision-making processes, risk management, or ethical deliberations. Key information such as training data, safety evaluations and governance rationales may or may not be disclosed.

(iii) **Licensing:** The company defines and enforces the terms under which contributions are accepted, retaining control over IP and the project's strategic direction. Even where open source licenses are used, the company typically manages key IP and licensing elements such as trademark, branding, and core model rights. Commercial terms in contributor licenses may restrict use by external stakeholders.

(iv) **Risk Management:** Ethics and risk management policies are developed and enforced internally, with little to no external input or transparency regarding their application. The company bears primary liability for any harm or misuse arising from the GenAI system, while external contributors face limited risk unless their submissions are infringing or malicious. The precise calibration of risk management responsibilities and distribution of liability need not follow a fixed blueprint. Rather, it is fundamentally shaped by the contractual terms that govern relationships between the company, external contributors, and end users.

Considerations in relying on Private Company Led Governance:

- Primarily operated by internal teams.
- Commercial applications of GenAI system a priority and hence licensing restrictions on use by external stakeholders
- Distribution of liability subject to contractual terms with external stakeholders
- Generally used in systems that are ready for end user deployment

b. Dual License or Open Core Governance:

This is a model where a company offers a permissively licensed open source core (e.g. basic models or tools) while retaining proprietary control over premium features, usage at scale, or commercial rights via a separate license or paid tier. Governance remains

firmly corporate-led, though a community may engage with the open core. Monetization is layered on top of the open core.

(i) Role Allocation: Users and contributors can interact with and sometimes contribute to the open core. Core proprietary features (e.g. enterprise APIs, advanced models, commercial access) are off limits to the community. Community contributions influence only the open core portion and rarely affect commercial features.

(ii) Transparency: Open core code is publicly visible and contributions are accepted. However, opaque governance covers premium tiers, licensing changes and policy decisions. The company may also reserve the right to change license terms and with it the kinds of information that may be published.

(iii) Licensing: Basic models or tools are released under permissive licenses (e.g. Apache 2.0, OpenRails). A separate proprietary license governs advanced features or commercial usage. The two tier licensing framework enables free open licensing for the open core, whereas a more restrictive commercial license governs enterprise usage.

(iv) Risk Management: The open core is open to external contribution and risk mitigation on this layer may be a shared between external contributors and internal teams. Liability for risks in the open core may also be distributed based on the role played by external contributors. However, policies governing commercial use are managed internally with no external oversight. Risk mitigation for the proprietary layer is similar to Private Company Led Governance.

Considerations in relying on Open Core or Dual Licensing:

- Proprietary license a key consideration, acting as a gatekeeper between "open" and "closed" parts of the GenAI system by defining what can be assessed, adapted, redistributed
- Liability risk subject to contractual terms and based on the role played by external stakeholders
- Used in GenAI systems that are in development, where certain use cases may require community input

c. Controlled Community Governance:

A hybrid model where corporate-sponsored projects are governed via semi-open governance structures. The project is governed via foundations or multistakeholder steering committees. This allows more external input as opposed to fully proprietary

models, while retaining corporate leadership. A controlled community governance framework blends corporate leadership with structured community involvement through neutral governance bodies. Multistakeholder governance bodies oversee governance, but the corporation(s) retain a strong influence in decision making. However, the corporation does not exercise unilateral control.

(i) **Role Allocation:** A decentralised form of governance as compared to the Private Company Led and Dual Licensing models. The Executive Committee comprising representatives from each domain-specific committee and key stakeholders holds ultimate accountability for governance strategy and coordination across domains. Unlike centralised models, this Executive Committee cannot make unilateral decisions but must build consensus across the distributed governance structure. Domain-specific committees establish and enforce governance principles in their respective areas (e.g., ethics, fairness, safety, transparency, data privacy), while external contributors propose code, flag risks, and participate under defined contributor license agreements.

(ii) **Transparency:** All committee meetings are documented and made publicly accessible, with open decision-making processes and structured feedback channels for community input. Transparent reporting and public engagement mechanisms ensure stakeholders can scrutinise governance actions and raise concerns effectively.

(iii) **Licensing:** Permissive open source licenses (e.g., MIT, Apache 2.0) are used to facilitate broad use, modification, and redistribution, with contributors retaining copyright but granting wide rights through project-approved licenses. Specialised IP and licensing committees regularly review and enforce licensing terms, ensuring compliance and clarity for all contributors.

(iv) **Risk Management:** The Executive Committee is responsible for oversight failures and ensuring due diligence in public feedback and conflict disclosure. Domain-specific expert committees address risks in relation to their areas of expertise. External contributors may be liable for introducing vulnerabilities or bias. Deployers are accountable for harm caused by deploying AI systems in sensitive contexts without appropriate safeguards or for misuse by end users.

Considerations in relying on Controlled Community Governance:

- Community input an essential part of the product development cycle. Opening up to a wider group of developers may play a role in expanding user base.
- Company's role is strategic: Exercising overall project oversight, enforcing compliances and taking a call on commercial end use
- Distributed liability risk between community and company. Requires more resources to drive community compliance and risk mitigation

d. Foundation Backed Governance:

In this model, a neutral non-profit foundation stewards and governs AI projects, while corporate sponsors contribute funding, technical resources, and participate in governance—but do not retain unilateral control. This model blends shared governance, high transparency, and multi-stakeholder engagement, with corporations supporting decision making.

(i) **Role Allocation:** The foundation's board sets the strategic vision, approves budgets, and ensures alignment between the project's mission and corporate interests. Core contributors manage technical direction and code quality. Development is community driven, with contributors from companies, academia, and open source developers. Working groups, special interest groups, or technical advisory committees coordinate development and make decisions on the features of the AI system. Companies participate as equals alongside other organisations in governance and technical roles.

(ii) **Transparency:** Governance documents, meeting minutes, and policy decisions are made publicly available, ensuring clarity on processes and contributor rights. Transparent documentation and open communication are aimed at building accountability and to enable scrutiny of project by external stakeholders.

(iii) **Licensing:** Standard permissive open source licenses (e.g., Apache 2.0, Berkeley Software Distribution (BSD), and Community Data License Agreements (CDAL)) are used, with contributor license agreements and IP policies clearly defining rights and obligations. The foundation manages IP ownership and licensing terms. Contributor License Agreements (CLAs) and IP policies used to clarify rights and responsibilities of external contributors.

(iv) **Risk Management:** Often includes dedicated Responsible AI working groups or a "Trusted AI" committee that maintains ethical guidelines and tool standards. The foundation and corporate sponsors are liable for oversight failures or harmful contributions. Core and external contributors face defined risks for introducing infringing or incompatible code or data. Deployers are likely to be exposed to secondary liability if end users use GenAI models for illegal or unethical purposes.

Considerations in relying on Foundation Backed Governance:

- Foundation is the primary decision maker and plays an important role in building trust with community
- Company's goals must be aligned with foundation, especially when it comes to commercial end use
- Built in risk mitigation with multiple stakeholders and committees responsible for enforcing compliance and minimizing risks in product development and deployment

IV Takeaways: Competing Considerations of "Openness"

As highlighted throughout this Playbook, open source AI has different meanings in different contexts and for different layers of a GenAI system. Our survey of different governance models in Section III also highlighted the competing considerations at play in how open a GenAI system is. While the benefits of an open source AI system are apparent, the decision on how open a GenAI system must be is a subjective determination that must be made at a project level. The table below summarises the key considerations at play in choosing a particular model for governance for an AI project.

Figure3: Comparison of Governance Models

Governance Model	Role Allocation	Transparency	Licensing	Risk Mitigation
Private Company Led	Key functions run by internal teams	Limited public access	Proprietary licenses with limitations on commercial use	Subject to contractual terms with external stakeholders
Open Core/ Dual Licensing	Core model open to community. Proprietary layer managed by internal teams.	Open core accessible to the public. Proprietary layer has multiple tiers of access	Open source licenses for open core. Proprietary layer governed by commercial license	Distributed liability risk for open core. Proprietary layer similar to Private Company Led Governance
Controlled Community	Decentralised communities manage the project. Company retains oversight.	Transparent reporting practices to promote community engagement	Open source licenses for community. IP committees decide commercial use cases.	Distributed across centralised executive committee, specialised communities and other contributors.
Foundation Backed	Managed by non-profit with community and private company(ies) participation. Company does not retain unilateral control	Transparent reporting practices to promote community engagement and oversight	Open source licenses. Foundation manages licensing terms for contributors.	Dedicated working groups and committees for risk mitigation

The decision to choose a particular model of governance is driven by the characteristic features of each project. As discussed in Section III, underpinning each model are competing concerns over commercialization, risk and control. Outlined below are key considerations in determining how open a GenAI system should be.

a. Commercialization

When and how to commercialise is an important consideration in the level of openness in an AI product cycle. A product that is ready for deployment to end consumers may see many of its governance functions internalised (e.g. Private Company Led Governance). However, projects that require community input or seek external oversight through the course of product development may choose to keep some parts of their GenAI systems open to community input (e.g., Dual Use Licensing). It is not uncommon for an AI project to start off with open source models and pivot to a more closed system as it approaches the end of a product cycle.[13]

b. Openness v Risk

As noted in our discussion in Section II, opening a GenAI system to external stakeholders can also increase the risk of external threats. Therefore, the level of openness of a GenAI system is also determined by the risk mitigation strategies in use. While community led risk mitigation models exist (e.g., Foundation Backed or Controlled Community Governance), companies may decide a particular strategy based on the level of oversight they choose to exercise. Opening up a GenAI system for community participation would necessarily mean a greater focus on enforcing compliance, clearcut liability frameworks for external stakeholders and setting up mechanisms to moderate the community.

c. Shared Governance

No GenAI system is a fully "closed" ecosystem. As noted in Section III, even centralised AI systems release some components of their GenAI systems under open licenses. This means that shared governance is an integral part to any open source AI system. Shared governance helps fosters transparency, accountability, and broad community involvement. By involving a diverse community of external stakeholders in decision-making processes, shared governance helps mitigate biases, anticipate unintended consequences, and build trust in the technology.

However implementing a particular shared governance strategy is determined by the level of control a company may choose to exercise in an AI project. This can range from internalizing governance functions in the case of Private Company Led Governance to outsourcing governance to an external stakeholder in the case of Foundation Backed Governance models. As noted in para IV (a) above, considerations with respect to commercialization may also be a determinant in the level of shared governance in an AI project.

[13] *See for instance, Stability AI's multi-tiered licensing for different use cases, available at <https://stability.ai/news/introducing-stability-ai-membership>.*

About Shardul Amarchand Mangaldas & Co:

Shardul Amarchand Mangaldas & Co. (SAM), founded on a century of legal achievements, is one of India's leading full-service law firms with the ISO/IEC 27001:2022 certification - the latest global benchmark for Information Security Management Systems. The Firm's mission is to enable business by providing solutions as trusted advisers through excellence, responsiveness, innovation, and collaboration. SAM is known globally for its exceptional practices in mergers & acquisitions, private equity, competition law, insolvency & restructuring, dispute resolution, international commercial arbitration, capital markets, banking & finance, tax, intellectual property, data protection and data privacy, white collar crime, technology law and infrastructure, energy and project finance.

With the full suite of Harvey AI functionalities, the Firm has a pan-India presence and has been at the helm of major headline transactions and litigations in all sectors, besides advising major multinational corporates on their entry into the Indian market and their business strategy. Currently, the Firm has over 800 lawyers including 188 Partners, offering legal services through its offices in New Delhi, Mumbai, Gurugram, Ahmedabad, Kolkata, Bengaluru, and Chennai.

About ASSOCHAM

The Associated Chambers of Commerce & Industry of India (ASSOCHAM) is the country's apex national chamber since 1920. It advocates actionable policy suggestions to strengthen the Indian economy by leveraging its extensive membership reach of over 450,000 companies, comprising of large corporates and SMEs. With over 70 Sector and State Councils, ASSOCHAM effectively represents diverse segments of Indian industry and focusses on aligning industry priorities with the nation's growth aspirations.

ASSOCHAM Contacts

Varun Aggarwal
Sr. Director & HOD-ICT
varun.aggarwal@assocham.com

Vicky Pandita
Dy. Director
ASSOCHAM
vicky.pandita@assocham.com

The Associated Chambers of Commerce and Industry of India

ASSOCHAM Corporate Office:

4th Floor, YMCA Cultural Centre and Library Building,
01, Jai Singh Road, New Delhi - 110001 • Ph: 011-46550555
Email: info@assocham.com • Website: www.assocham.org