Shardul Amarchand Mangaldas

A DECADE YOUNG, A CENTURY STRONG

#BHARAT FOR AI

Enabling Frameworks for Trust

EDUCATION, DEFENCE, GOVERNANCE, AGRICULTURE AND CAPACITY-BUILDING

Foreword

AI has become the defining general-purpose technology of our era, reshaping how industries create and deliver value. The unique features of AI - agility, proximity to users and speed—empower businesses to build robust and reliable solutions for business growth. However, with technological scale and diffusion come commensurate risks; and only a principles-based approach, grounded in lawfulness, accountability, transparency, privacy and human oversight can convert such innovation into sustainable adoption.

In lockstep with this vision, it brings us great pleasure to present this publication, "**Bharat for AI: Enabling Frameworks for Trust**" on the culmination of the India–AI Impact Summit 2026 —the first global AI summit hosted in the Global South, convening governments, industry, researchers, and civil society. The Artificial Intelligence and Emerging Technology Team at Shardul Amarchand Mangaldas & Co. ("**SAM**") has developed this series, advancing the discourse on AI governance, regulation, and responsible deployment in India.

This publication draws its orientation from India's Artificial Intelligence Governance Guidelines—the framework charting approaches for a balanced, agile, and pro-innovation course for AI development. Across these essays, we operationalise the sutras of India's approach, advancing a risk-based framework that prioritises voluntary compliance and proportionate safeguards. As AI's transformative potential sharpens, the Summit crystallises this pivotal moment- buttressing the need to address distinct questions of trust, data, computation, and institutional readiness.

This series responds to the need of charting practical pathways for governance, deployment, and sectoral transformation. Animating our work is a #BharatforAI perspective: AI governance that is pragmatic, implementable, and aligned with international norms. It suggests strengthening existing legal remedies, targeted risk-based institutions, and a careful equilibrium between public interest, innovation, and enforceability— to encourage compliance and cross-border cooperation.

Through focused analysis of sector-specific technologies in defence, education, and agriculture, and of the pressing needs for governance and capacity building, these five essays are intended to guide decision-makers toward workable safeguards for AI systems.

We hope this work serves to channel a powerful current of innovation into safe harbours of trust and long-term value.

Yours sincerely,
Dr. Shardul S. Shroff
Executive Chairman and Founder,
Shardul Amarchand Mangaldas & Co.

Table of Contents

Main Messages

As artificial intelligence (“**AI**”) rapidly transforms the fabric of India’s economy and society, the question of legal responsibility for AI-driven harms has become both urgent and complex. The integration of AI into critical sectors—ranging from healthcare and finance to defence and public services—has outpaced the evolution of India’s legal and regulatory frameworks.

Bharat for AI is premised on a foundational conviction: India’s AI trajectory must be shaped by both technological ambition and robust institutional, regulatory, and social architectures to ensure its sustainable success. This volume responds to these challenges through five essays, each examining the emerging challenges and opportunities of India’s AI ecosystem across critical domains—education, defence, governance, agriculture, and capacity-building. Through rigorous analysis and targeted recommendations, these essays offer a roadmap for policymakers, practitioners, and stakeholders committed to navigating the complexities of responsible AI adoption across the nation.

Chapter 1: Reliability Baselines for Education AI Deployments

- Education AI (“**EdAI**”) introduces a distinct class of reliability and safety risks that accumulate quietly and can become systemic over time. Learners often cannot detect confident errors; over time, this can normalise misconceptions. At the same time, always-on assistance may weaken productive struggle, shifting learning from active reasoning to cognitive offloading. Generative content pipelines can also drift from curricula, embed bias, and degrade the information environment, while cyber-enabled impersonation and data exposure threaten child safety and institutional trust.
- A defined reliability baseline for public EdAI deployments, encompassing pedagogical alignment, integrity in content generation and evaluation, and robust security-resilience standards.

Chapter 2: Trust and Safety Benchmarks for Defence Technology LLMs

- Defence technology systems employing Generative AI face an elevated likelihood of operational failure and legal non-compliance—stemming from inherent model limitations such as hallucinations and the high-stakes nature of military applications.
- A defence-specific benchmarking framework is proposed, grounded in three evaluative dimensions: (i) international humanitarian law and relevant jurisprudence, operationalising principles of legality, accountability, sovereignty, and human rights through metrics measuring legal adherence and output bias; (ii) municipal law compliance, including data privacy and criminal law, ensuring data provenance, protection, and legality; and (iii) trust and safety principles, emphasising data sovereignty and system reliability through metrics of accuracy, bias, and fairness.

Chapter 3: Joint Parliamentary Committee as an Instrument for AI Governance

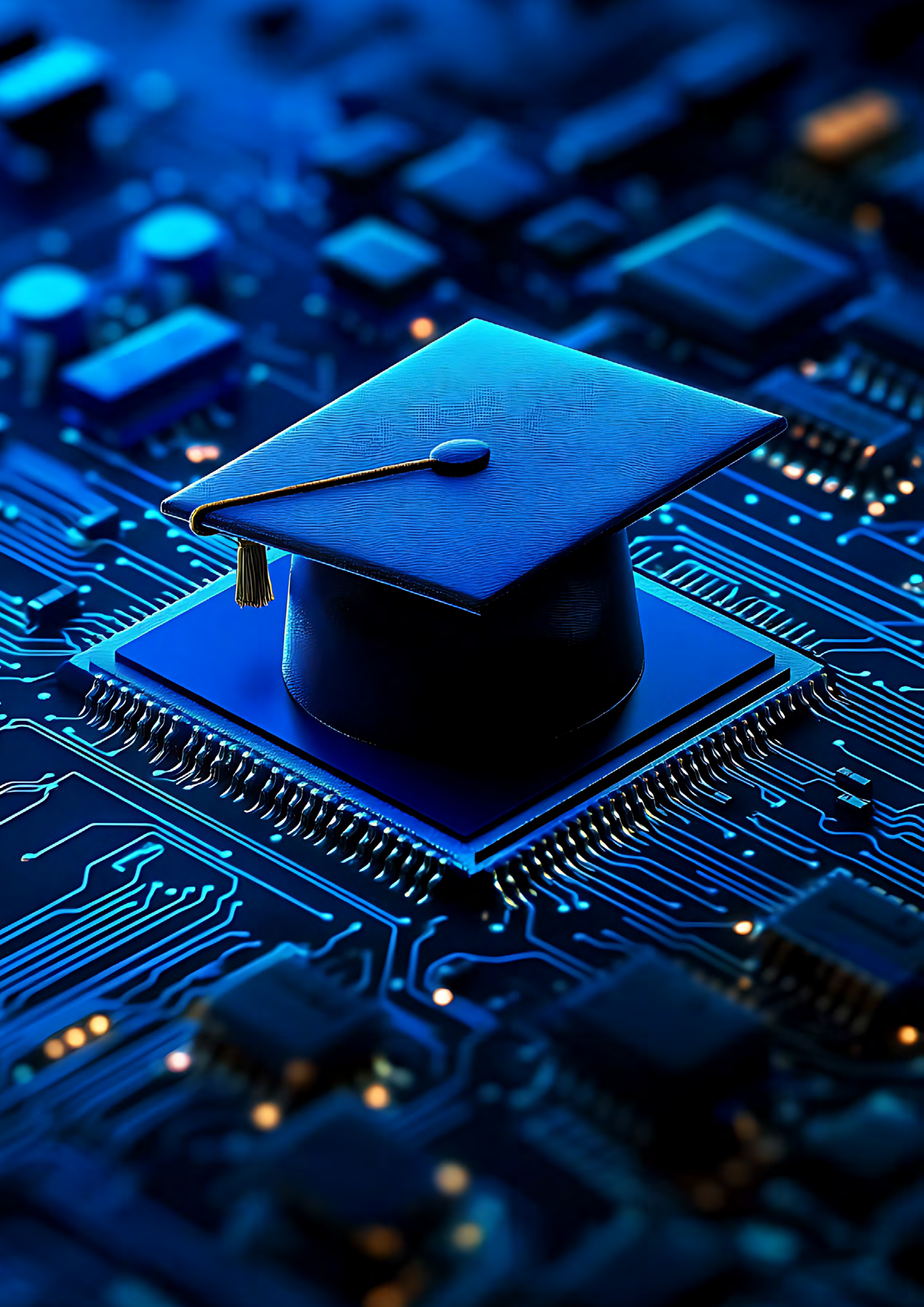
- India’s AI governance currently rests on a fragmented assemblage of Acts, Rules, advisories, national strategies, guiding principles, and sector-specific regulations. This piecemeal and largely reactive approach has attracted criticism for generating regulatory uncertainty and inadequately addressing emergent risks such as algorithmic bias, model drift, and synthetic media including deepfakes.
- A multipartisan Joint Parliamentary Committee (“**JPC**”) tasked with studying AI’s societal implications and developing a coherent regulatory framework. Leveraging its investigative powers and capacity for sustained technical inquiry, a JPC on AI can bridge the institutional gap between parliamentary oversight and executive action.

Chapter 4: National Framework for Agriculture Data Interoperability

- Despite vast quantities of agricultural data being collected across government departments, ministries, and private entities, no coherent data interoperability framework existsfor agricultural data. This absence has resulted in systemic heterogeneity in data maintenance, siloed application of standards, and semantic inconsistencies that undermine the efficacy of AI-driven solutions.
- A national framework for agricultural data interoperability, designed to achieve legal, organisational, technical, and semantic alignment across datasets. Such a framework would enable the harmonisation of data necessary to unlock the full potential of AI in Indian agriculture.

Chapter 5: Competency Framework for Upskilling Women in the AI Ecosystem

- Three structural barriers constraining women's participation in the technology sector,—(i) entry barriers (limited access to quality STEM education and biased recruitment practices), (ii) sustenance barriers (hostile workplace cultures, caregiving penalties, and persistent pay inequities), and (iii) progression barriers (restricted leadership pipelines and inadequate mentorship). Without deliberate and targeted intervention, AI technologies risk perpetuating and even deepening these entrenched inequalities.
- A "Gender-Responsive Competency Framework" for AI skilling, designed to address women's specific needs by aligning recruitment, training, mentoring, and workplace support incentives. This framework aims to ensure equitable access, retention, and advancement in the emerging AI economy, seizing the AI revolution as a transformative opportunity to dismantle deep-seated social constraints on women's workforce participation.



CHAPTER 1:

Reliability Baselines for Education AI Deployments

Introduction and Scope

Education is a fundamental human right and a central determinant of economic growth, social resilience, and technological progress. In a country where diversity, demographic scale, and entrenched developmental inequalities shape educational outcomes, the deployment of digital tools constitutes a significant pathway to reducing learning disparities. As connectivity grows and digital innovation accelerates, integrating technology into education is increasingly integral. Accordingly, the central task is to advance these aims while maintaining equity, ensuring quality, and protecting learners. Artificial Intelligence (“**AI**”) is now a major part of this shift, encompassing tools that support tutoring, practice, educational content (“**content**”) development, translation, and classroom administration.[1]

For the purposes of this essay, Education AI (“**EdAI**”) refers to AI-enabled systems that ingest, generate, adapt, translate, or evaluate content, and facilitate interactions for learners, teachers, and administrators. India’s public education system is scaling digital learning across curricula, education boards, and languages, within classrooms marked by uneven foundational skills, uneven device access, and limited supervision.[2] As an illustration, learners routinely ask questions in Hinglish and other mixed-code forms; if a model misconstrues the prompt or mis-parses these multimodal or mixed-code inputs and responds with high confidence, misconceptions can become normalised.[3] Similarly, if institutions rely on AI-generated content without continuous verification and curriculum alignment, small inaccuracies and content drift can accumulate and entrench misalignment at scale.[4] Over time, these dynamics can weaken learning outcomes, undermine safety, and erode institutional trust, making reliability a precondition for sustainable innovation at scale. Within this broader digitisation trajectory, AI emerges as a distinct capability layer that carries materially higher reliability and safety risks.

Education AI: Capabilities and Risks

Education-focused AI is increasingly being integrated into public education systems through government-led partnerships with platform providers and frontier model developers.[5] In this framing, the main emerging decision-makers are learners, teachers, parents, and institutions; accordingly, this section categorizes EdAI by stakeholder function as learner-facing, teacher-facing, and institution-

[1] See notable tools: Duolingo Max uses OpenAI’s GPT-4 for interactive conversation practice (Video Call, Roleplay), with feedback and transcripts for review (https://blog.duolingo.com/duolingo-max/). Gemini in Classroom offers 30+ AI tools (e.g., lesson outlines, quizzes, re-level text) (https://blog.google/products-and-platforms/products/education/classroom-ai-features/). Achievements include ML models that infer a protein’s 3D structure from its amino-acid sequence, enabling protein engineering (The Royal Swedish Academy of Sciences, *Nobel Prize in Chemistry 2024* press release, https://www.nobelprize.org/prizes/chemistry/2024/press-release/) accessed Jan 2026.

[2] ASER Centre’s *Annual Status of Education Report 2023*, https://asercentre.org/wp-content/uploads/2022/12/ASER-2023_Main-findings-1.pdf reports that ~1 in 4 rural youth (14–18) cannot fluently read a Std II text in their regional language, and only 43.3% can solve a 3-digit ÷ 1-digit division problem (Std III/IV level) accessed Jan 2026.

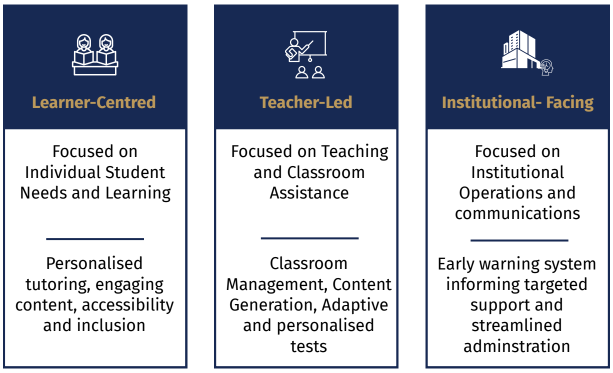
[3] See HiACC (Hinglish adult & children code-switched corpus) (https://pmc.ncbi.nlm.nih.gov/articles/PMC12329218/): code-switching—“the frequent alternation between two or more languages within a single utterance”—is widespread in India; the paper estimates 250M+ people use code-switched communication (notably Hinglish) and finds monolingual-trained models underperform by ~42% WER, implying Indian-realistic inputs (Hinglish, local phrasing, variable literacy) can trigger reliability failures when evaluation data is primarily monolingual or otherwise unrepresentative. In parallel, the OECD *Digital Education Outlook 2026: Exploring Effective Uses of Generative AI in Education* (https://doi.org/10.1787/062a7394-en) cautions that outsourcing cognitive tasks to general-purpose GenAI may improve task performance without learning gains and can reduce sustained engagement over time. These risks scale in a vast, heterogeneous school system: see PIB, Ministry of Finance, Government of India (2025), *Economic Survey 2024–25* (https://www.pib.gov.in/PressReleasePage.aspx?PRID=2097864&reg=3&lang), where the survey and the current digital divide (e.g., state-level experience in Tamil Nadu) underscore uneven readiness; illustratively, in 2023–24 only 53.9% of schools had internet access and 57.2% had computer access (with improvements reported the following year) accessed Jan 2026.

[4] See Doewes & Pechenizkiy (2021) (https://educationaldatamining.org/EDM2021/virtual/static/pdf/EDM21_paper_243.pdf) The first cautions against treating AI-based assessment as a drop-in substitute for teacher judgment: human–computer agreement can overstate reliability, and essay-scoring systems that “match humans” can still fail under realistic input shifts (e.g., off-topic, nonsensical, or paraphrased responses). The U.S. Department of Education (2023) (https://www.ed.gov/sites/ed/files/documents/ai-report/ai-report.pdf) policy similarly emphasizes AI as support—not replacement—for high-quality, human-led formative assessment, and calls for inspectable, explainable systems. Lastly, UNESCO (2023) (https://unesdoc.unesco.org/ark:/48223/pf0000386693/PDF/386693eng.pdf.multi) warns that generative AI can create recursive risks as AI-generated text enters future training data, and may narrow plural opinions and ideas. accessed Jan 2026.

[5] OpenAI, Introducing ChatGPT Edu (2024). https://openai.com/index/introducing-chatgpt-edu/; OpenAI. Introducing OpenAI’s Education for Countries. (2025) https://openai.com/index/edu-for-countries accessed January 2026.

facing tools. Figure maps EdAI tools by stakeholder and highlights key use cases for each.[6] *(Refer Illustration: 1)*

Illustration 1: Education AI: Key Stakeholders and Focus



Learner-Centred

Focused on Individual Student Needs and Learning

Personalised tutoring, engaging content, accessibility and inclusion

Teacher-Led

Focused on Teaching and Classroom Assistance

Classroom Management, Content Generation, Adaptive and personalised tests

Institutional- Facing

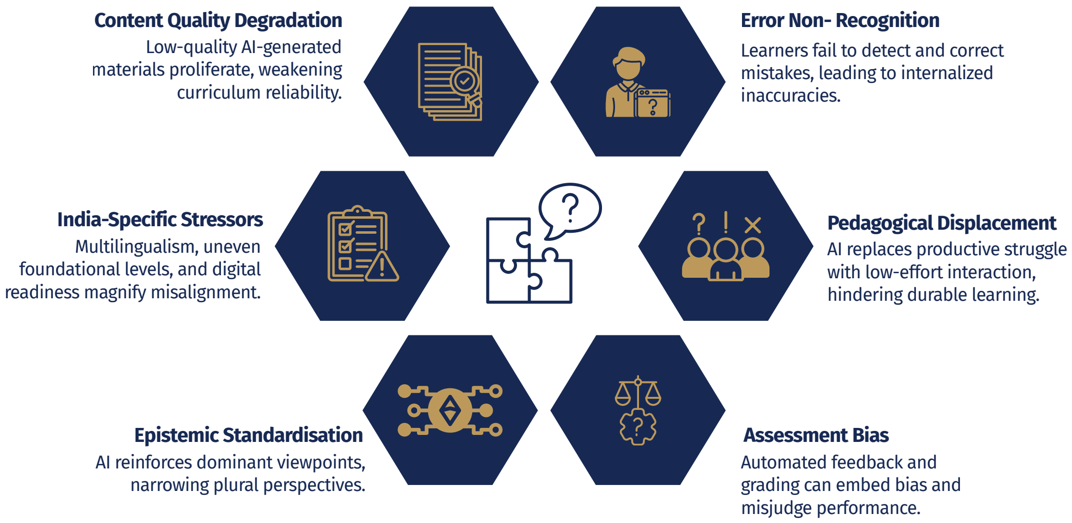
Focused on Institutional Operations and communications

Early warning system informing targeted support and streamlined adminstration

- **Learner-facing EdAI** (especially intelligent tutoring systems) may personalise pace, difficulty, and feedback in real time, helping learners catch up or extend learning through one-to-one support. In addition, AI may generate more engaging and contextually relevant content, supporting deeper understanding across varied learner backgrounds. AI has also been projected to reduce barriers for diverse learners by supporting multilingual rewriting and clarification; providing assistive features for disabilities and special education needs; lastly, chatbots can also expand access to information and basic support.[7]
- **Teacher-facing EdAI** (including social and assistive help-bots) may support classroom management and help curate, adapt, and diversify learning materials, improving language and cultural accessibility while reducing preparation burdens where resources are constrained. Alongside this, rubric-aligned feedback and automation of routine tasks (for e.g., assigning adaptive worksheets) improve consistency, freeing teacher time for higher-value instruction.[8]
- **Institution-facing EdAI** may support system-level decision-making by identifying patterns associated with disengagement or dropout risk, enabling earlier, better-targeted interventions and more efficient allocation of support and resources. Complementarily, it may streamline routine documentation, reporting, and workflow coordination, reduce administrative load while enabling real-time status updates, surfacing bottlenecks early to support faster and more consistent response.[9]

This stakeholder-function typology delineates where EdAI delivers value and where failures may emerge and scale in public deployments. A central failure mode is error opacity: learners often cannot recognise when outputs are wrong. Learners may over-rely on confident outputs, overestimate their ability to detect errors, apply weak verification

Illustration 2 - Challenges in EdAI Deployment



Content Quality Degradation
Low-quality AI-generated materials proliferate, weakening curriculum reliability.

Error Non- Recognition
Learners fail to detect and correct mistakes, leading to internalized inaccuracies.

India-Specific Stressors
Multilingualism, uneven foundational levels, and digital readiness magnify misalignment.

Pedagogical Displacement
AI replaces productive struggle with low-effort interaction, hindering durable learning.

Epistemic Standardisation
AI reinforces dominant viewpoints, narrowing plural perspectives.

Assessment Bias
Automated feedback and grading can embed bias and misjudge performance.

[6] Source- Authors

[7] Organisation for Economic Co-operation and Development. (2024, August). *The potential impact of artificial intelligence on equity and inclusion in education* https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/08/the-potential-impact-of-artificial-intelligence-on-equity-and-inclusion accessed Jan 2026

[8] Organisation for Economic Co-operation and Development. (2021). *OECD Digital Education Outlook 2021: Pushing the frontiers with artificial intelligence, blockchain and robots*. OECD Publishing. https://doi.org/10.1787/589b283f-en ; Organisation for Economic Co-operation and Development. (2024, August) *The potential impact of artificial intelligence on equity and inclusion in education* https://www.oecd.org/content/dam/oecd/en/publications accessed January 2026

[9] Organization for Economic Co-operation and Development. (2024, August). *The potential impact of artificial intelligence on equity and inclusion in education* https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/08/the-potential-impact-of-artificial-intelligence-on-equity-and-inclusion accessed January 2026

practices (including “checking AI with AI”), and internalise incorrect facts or reasoning as knowledge. At the same time, studies increasingly indicate that EdAI risks are not limited to factual errors but also arise from learners' interaction patterns. While human tutors often employ Socratic questioning patterns that stimulate active thinking, AI systems can default to passive “explanation–response” loops in which the model delivers information and the learner engages minimally.[10] Although learners achieve better immediate results, over time this does not produce durable learning and can reduce cognitive stamina, deep reading, sustained attention, and perseverance.[11] Figure summarises the principal challenge vectors for public EdAI deployments, including content quality degradation, error non-recognition, pedagogical displacement, epistemic standardisation, assessment bias, and India-specific stressors.[12] *(Refer Illustration: 2)*

Three system-level risks are especially salient for public deployments. ***First***, AI displaces the “productive struggle” essential for learning: the sustained effort through which learners practise reasoning, surface misconceptions, and consolidate understanding.[13] This may shift classrooms towards engagement-optimised and commercially driven interactions over learning gains. Such pedagogical misalignment can produce systematic, self-reinforcing, and long-lasting impacts.[14] ***Second***, as AI-generated lessons proliferate online, they introduce long-horizon integrity risks. When such material is later scraped into training corpora for subsequent models, embedded inaccuracies and biases can recur and compound across model generations, progressively degrading educational content reliability. In particular, because these systems are opaque, they may also standardise dominant viewpoints, particularly in the social sciences—, and embed biased evaluation patterns that are difficult to detect, contest, or correct.[15] ***Third***, AI lowers the barrier to targeted phishing and impersonation of learners (for example, convincing messages “from a teacher” or “from the school”), enabling coercion, bullying, or reputational harm.[16]

Once EdAI is embedded in content pipelines, assessment workflows, and platform infrastructure, these risks can rapidly become systemic. Accordingly, their likelihood, scale, and reversibility depend on the governance and infrastructure through which EDAI is procured, integrated, and monitored: making India's digital education architecture the next necessary point of analysis.

India's Digital Education Architecture And The Case For An EdAI Reliability Baseline

India's constitutional design places education on the Concurrent List, while vesting the Union with standards-setting authority for higher education and research institutions.[17] As a result, Educational Technology (“**EdTech**”) products are governed through a combination of sector-specific education instruments and cross-cutting digital regulation applicable to platforms, data processing, and online safety.[18] Prominently, this includes the National Education Policy 2020 (“**NEP 2020**”) as the overarching

[10] TEAS: *Trusted Educational AI Standard: A Framework for Verifiable, Stable, Auditable, and Pedagogically Sound Learning Systems* https://doi.org/10.48550/arXiv.2601.06066, accessed January 2026

[11] Schleicher, A. (2026, January 19). *How to effectively use Generative AI in education. OECD* Blogs. https://www.oecd.org/en/blogs/2026/01/how-to-effectively-use-generative-ai-in-education.html; accessed January 2026

[12] Source- Authors

[13] *Ibid*.

[14] TEAS: Trusted Educational AI Standard: A Framework for Verifiable, Stable, Auditable, and Pedagogically Sound Learning Systems https://doi.org/10.48550/arXiv.2601.06066, accessed January 2026

[15] UNESCO. (2023). *Guidance for generative AI in education and research* https://unesdoc.unesco.org/ark:/48223/pf0000386693/PDF/386693eng.pdf.multi Liang, W. X. et al. (2023). GPT Detectors Are Biased against Non-Native English Writers. *Patterns*, *4*, 100779.https://www.cell.com/patterns/fulltext/S2666-3899(23)00130-7?_returnURL=https%3A%2F%2Flinkinghub.elsevier.com%2Fretrieve%2Fpii%2FS2666389923001307%3Fshowall%3Dtrue Research has documented that AI-powered detection tools disproportionately falsely flag essays written by non-native English speakers as AI generated, creating significant risks of false academic dishonesty accusations for this population accessed Januray 2026

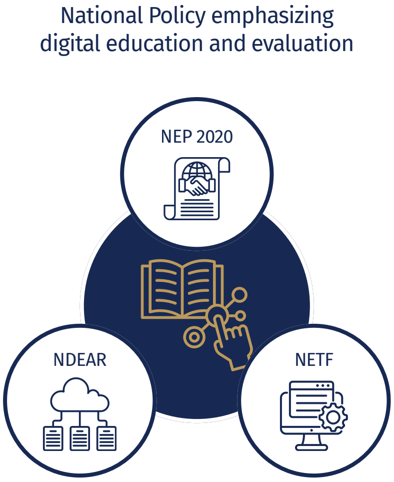
[16] UNESCO. (2023). Guidance for generative AI in education and research https://unesdoc.unesco.org/ark:/48223/pf0000386693/PDF/386693eng.pdf.multi accessed January 2026

[17] *See* Ministry of External Affairs, Government of India, Seventh schedule (Article 246), List I, Entry 66 and List III, Entry 25 https://www.mea.gov.in/images/pdf1/S7.pdf accessed January 2026

[18] Most “horizontal” digital rules chiefly govern lawful data processing, cyber incident readiness, and platform due diligence, and are therefore not determinative for a reliability baseline focused on pedagogy-, curriculum-quality, or learner-safety outcomes. This includes the Digital Personal Data Protection Act, 2023 and DPDP Rules, 2025 (lawful personal-data processing, including children safeguards) https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf; CERT-In Cyber Security Directions (incident readiness/reporting and logging duties) https://www.pib.gov.in/PressReleasePage.aspx?PRID=1820904&; and the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (platform due diligence for user content) https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf. Likewise, consumer-facing EdTech measures focus on market conduct (pricing/marketing/deceptive practices, grievances), not learning-behaviour correctness or curriculum-integrity baselines: Ministry of Education advisory cautioning citizens regarding EdTech companies https://www.pib.gov.in/PressReleasePage.aspx?PRID=1784582& and PRAGYATA: Guidelines for Digital Education (active supervision, bounded screen-time, and checks on content quality/syllabus alignment) https://www.education.gov.in/sites/upload_files/mhrd/files/pragyata-guidelines_0.pdf. Finally, the RTE, 2009 https://www.education.gov.in/sites/upload_files/mhrd/files/upload_document/rte.pdf establishes education as a fundamental right, while national platforms advance access objectives (e.g., SWAYAM; e-Pathshala for NCERT/CIET multilingual resources; DIKSHA for curriculum-linked school content). See also Meena, N. (2025). *International Journal of Political Science and Governance*, “Shaping the future of education in India”: https://doi.org/10.33545/26646021.2025.v7.i7a.587. accessed Jan 2026.

policy direction, the National Educational Technology Forum ("**NETF**") as the principal standard-setting platform guiding technology integration, and the National Digital Education Architecture ("**NDEAR**") as the interoperable digital infrastructure for adoption across States and platforms.[19] Figure illustrates principal pillars of India's digital education architecture relevant to EdAI adoption, enablement and governance.[20] (*Refer Illustration 3*)

Illustration 3 - Prominent Pillars of India's Digital Education Architecture



The NEP 2020 identifies digital education as a reform priority, while explicitly recognising its potential risks. It calls for rigorous evaluation and appropriately scaled pilots for emerging and disruptive technologies.[21] It envisages the NETF as the institutional mechanism to support evidence-based induction, deployment, and use. NETF is intended to serve as a central advisory platform for education leadership and governments by sharing best practices, recommending interoperable open solutions, and advancing national data and translation initiatives (e.g., ONOD and Anuvadini).[22]

Complementarily, NDEAR is a technological framework designed to enable "an open, evolvable, public digital infrastructure."[23] It provides interoperable building blocks for reuse across the education ecosystem and is intended to catalyse innovation and support the timely implementation of policy goals.[24] The NDEAR Open Standards and Specifications further elaborate expectations for APIs, open-source components, and sandbox environments to support interoperability across Centre, State, and school-level applications.[25] Together, these instruments provide a strong foundation for scale and interoperability of AI integrated EdTech products.

However, the scale and functional profile of EdAI introduce reliability risks that enablement and evaluation-oriented governance does not fully address. In public deployments, where education delivery is a core state responsibility, reliability duties must be specified not only for adoption, but for sustained behaviour: whether systems remain consistently learning-appropriate, whether content and evaluation outputs remain dependable over time, and whether deployment is resilient to misuse and compromise. This governance need is most salient across three vectors.

a. ***Cognitive offloading and Pedagogy Misalignments:*** Today digitalization and AI remain an unrealised pedagogical promise.[26] The UNESCO AI Competency Frameworks emphasise human-centered approaches, critical thinking,

[19] Also see PIB (2025), Economic Survey 2024–25: India's school education system (https://www.pib.gov.in/PressReleasePage.aspx?PRID=2097864&reg=3&lang=2), which notes that the Government is pursuing NEP 2020 objectives through a range of programmes and schemes. accessed Jan 2026.

[20] Source- Authors

[21] See National Education Policy 2020 (Chs. 23–24), which notes that "data is a key fuel for AI-based technologies," urges awareness on data handling and ethical issues in AI deployment, and calls for eliminating the "digital divide" (Ministry of Human Resource Development, Government of India, https://www.education.gov.in/sites/upload_files/mhrd/files/NEP_Final_English_0.pdf, accessed Jan 2026.

[22] See PIB, Ministry of Education, "National Digital Education Architecture (NDEAR) to be set up" (2021) (https://www.pib.gov.in/PressReleasePage.aspx?PRID=1696880&lang=2&reg=3) and NETF (https://netf.aicte-india.org/about-netf.html; https://netf.aicte-india.org/major-initiatives.html). NETF initiatives include One Nation One Data (a unified education-data access point enabling user-consented sharing via "2-way Open APIs") and Anuvadini (an AI text/voice translation tool supporting 22 languages, including text, speech, and video translation, with "GPT Integration") accessed Jan 2026

[23] PIB, Ministry of Education, "Technical Learning Facilities" (2021) https://www.pib.gov.in/PressReleasePage.aspx?PRID=1783481 accessed Jan 2026.

[24] Ministry of Education, *NDEAR Ecosystem Policy* (2022) (https://www.ndear.gov.in/images/pdf/NDEAR-Ecosystem%20Policy-Version.pdf) operationalises NDEAR through interoperable "building blocks"—self-contained capabilities exposed via open APIs—so platforms can plug into shared foundational services rather than rebuild them. It structures ecosystem participation through Use / Contribute / Enlist, and distinguishes (i) Core and Common Building Blocks (API services, and optionally applications) that require approval and ongoing compliance, from (ii) Reference Building Blocks (open-source code, specifications, data, assets, and models) that are openly accessible without approvals. For Core/Common integration, it sets baseline conditions including government-notified API security practices, compliance with the IT Act, 2000 and applicable personal-data/privacy requirements, telemetry sharing per specifications, authority to revoke access for misuse or terms violations, and requirements to provide a sandbox environment and documentation for testing open APIs. accessed January 2026.

[25] See Ministry of Education, *Open Standards & Specification for NDEAR* (2022) (https://www.ndear.gov.in/images/pdf/NDEAR-Open%20Standards_Version.pdf), which sets out the technical architecture: 12 building-block categories and 36 minimum viable building blocks, designed as loosely coupled components connected through standardised APIs and open specifications. The 12 categories are: Open Standards & NDEAR Portal; Federated Identities; Reference Data; Infrastructure; Technology; Governance; Administration; Content; Learning; Reference Solutions UX; Open Data & Analytics; and Ecosystem Sandbox. accessed January 2026.

[26] See OECD (2024), *Education Policy Outlook 2024: Reshaping teaching into a thriving profession from ABCs to AI* (https://doi.org/10.1787/dd5140e4-en). Cognitive offloading is the use of external aids to reduce a task's information-processing demands, and a tool is pedagogically misaligned when its default interactions optimise for "helpfulness" (speed, completion, fluency) rather than learning processes that build durable understanding (https://www.sciencedirect.com/science/article/abs/pii/S1364661316300985) accessed Jan 2026

and ethical considerations in developing AI-specific pedagogical skills.[27] Related approaches similarly propose leveraging AI for personalisation while requiring learner practices of attribution and reflection, to preserve agency.[28] Illustratively, field evidence in school-level mathematics suggests that a generic Generative Pre-trained Transformer ("**GPT**")-style tutor can raise performance in the time of assisted practice yet reduce performance once tool access is removed, indicating weaker underlying skill acquisition.[29]

Related experimental evidence finds that immediate assistance can shift learner's self-regulated learning away from generating, monitoring, and revising their own reasoning to outsourcing those metacognitive steps to the tool (planning what to write/solve, deciding next steps, and resolving uncertainty), so engagement and active diagnosis decreases. This displaces the steps to consolidate understanding; and over time, this leads to excess use and over-reliance.[30] While India's current framework supports evaluation and pilots, it remains under-specified on baseline requirements that ensure EdAI-mediated interactions reliably (consistent and verifiable manner) support learning transfer, cognitive endurance, and durable skill acquisition in public deployment conditions.

b. ***Content Quality Instability and Integrity:*** Generative systems can fail a core educational requirement: dependable knowledge. More precisely, as these models generate output by learning probabilistic patterns rather than by understanding or reasoning, they can produce text that appears credible while embedding errors, omissions, or bias.[31] UNESCO similarly cautions that such AI-generated content is increasingly spread online, degrading the quality of the information environment on which learners rely. A structural risk is the erosion of the long-tail educational content, i.e., niche or low-frequency topics outside mainstream curricula, which can be progressively omitted, diluted, or overwritten as high-frequency synthetic patterns accumulate and circulate.[32] This risk is salient in the humanities and social sciences, where materials essential for accurate, contextual understanding, including regionally specific histories, subaltern and tribal perspectives, local political movements, and nuanced policy debates may be marginalised in favour of widely represented narratives.

   The same tendency extends to evaluation: if assessment systems rely on opaque and biased criteria, they may reward conformity to dominant framings and penalise other well-grounded arguments, normalising unstable or inconsistent evaluation over time. Although India's digital education framework articulates quality and curriculum objectives, it remains under-specified for EdAI deployments' content risks of drift, bias, and integrity in AI content pipeline and evaluations. Accordingly, content-quality standards that ensure that degradation is continuously monitored and corrected, ensuring long term reliability across successive cohorts of models and knowledge bases**.**

c. ***Safety and Cyber-Resilience:*** Reliability is inseparable from operational security and child safety in this domain. In a high-threat environment, platform vulnerabilities, data exposure, and adversarial manipulation can directly erode trust in digital learning systems and create risks extending beyond learning outcomes.[33] Notably, reports of frequent cyber targeting of educational institutions, alongside incidents of exposure of personally identifying data on large-scale national education platforms, illustrate the urgent need to address security failures in education infrastructure.[34] Accordingly, any reliability baseline for EdAI in public deployments must incorporate cyber-resilience as a core operational condition.

[27] UNESCO., *Draft AI competency frameworks for teachers and for school students* [Draft report]. Retrieved February 3, 2026, from https://www.unesco.org/sites/default/files/medias/fichiers/2023/11/UNESCO-Draft-AI-competency-frameworks-for-teachers-and-school-students.pdf

[28] Verhoeven, B., & Hor, T. (2025, February 12). Human-Centric AI-First ("HCAIF"), *A framework for human-centric AI-first teaching*. AACSB. https://www.aacsb.edu/insights/articles/2025/02/a-framework-for-human-centric-ai-first-teaching accessed Jan 2026

[29] Bastani, "Generative AI Can Harm Learning" (SSRN, 2024) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4895486; accessed Jan 2026

[30] British Journal of Educational Technology, 2024) finds ChatGPT can promote dependence, improving short-term essay scores but not necessarily knowledge gain/transfer, https://bera-journals.onlinelibrary.wiley.com/doi/abs/10.1111/bjet.13544

[31] TEAS Framework Ibid.

[32] See UNESCO (2023), Guidance for generative AI in education and research (https://doi.org/10.54675/EWZM9535). A further integrity risk is model collapse under recursive training on synthetic/model-generated data: as models are trained (directly or indirectly) on model-generated text, they progressively lose information, with degradation beginning at the "tails" of the distribution (https://www.nature.com/articles/s41586-024-07566-y). This is especially salient for education's long-tail needs—low-frequency, niche, or local topics—which can be omitted or overwritten as high-frequency synthetic patterns accumulate (https://www.researchgate.net/publication/220040283_Minds_on_fire_Open_education_the_long_tail_and_learning_20. For a mainstream illustration of "long-tail" dynamics, see EAB's discussion of long-tail keywords in higher-education https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/08/the-potential-impact-of-artificial-intelligence-on-equity-and-inclusion

[33] See Elliott & Mehrotra (WIRED, Jan 23, 2023), reporting that a security lapse in DIKSHA—an Education Ministry app used nationwide—left an exposed cloud server that revealed students' and teachers' personal data for over a year. https://www.wired.com/story/diksha-india-education-app-data-exposure/ accessed January 2026

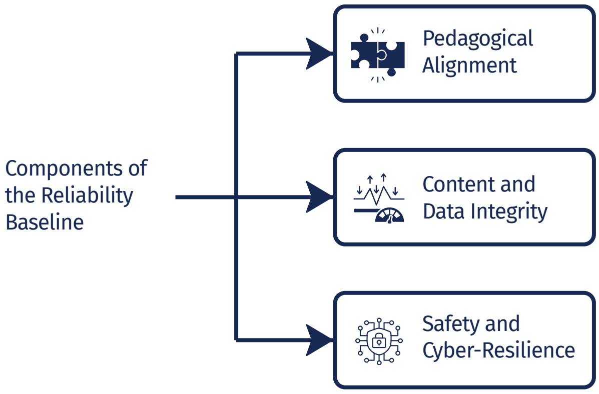
[34] See India Today (Aug 14, 2025) and *The Economic Times* (Aug 14, 2025), reporting a pilot study under CyberPeace Foundation's e-Kawach initiative ("Exploring Cyber Threats and Digital Risks to Indian Educational Institutions") that found Indian educational institutions faced 200,000+ cyberattacks and nearly 400,000 data breaches over a nine-month period (July 2023–April 2024): https://www.indiatoday.in/education-today/news/story/indian-education-sector-hit-by-2-lakh-cyberattacks-4-lakh-data-breaches; https://m.economictimes.com accessed January 2026

These vectors establish the need for Indian governance architectures to address new failures and risks for EdAI. The reliability baseline must define minimum duties for learning-appropriate behavior, content and evaluation integrity, and security-resilience in public deployments.

Setting Reliability as a Baseline for Public Deployments

India's EdAI deployment will be distributed across a vast and heterogeneous school system, serving approximately 24.8 crore students across 14.72 lakh schools, with uneven digital readiness and highly variable classroom conditions.[35] In this context, a reliability baseline is a precondition for safe and consistent scale across diverse classrooms. Within India's architecture, NETF should publish a minimum baseline definition of reliability for EdAI. Connectedly, the NDEAR should embed and promote these with ecosystem-participation for public deployments. The baseline should explicitly cover three dimensions: (a) pedagogical alignment (learning-appropriate behavior), (b) content and data integrity (curriculum alignment, provenance, accuracy, and quality standards for instructional content and evaluation), and (c) safety and cyber-resilience, as prerequisites for reliable operation. The figure displays the three components of the proposed EdAI reliability baseline.[36] (*Refer Illustration* 4)

Illustration 4 - Components of the Reliability Baseline


Components of the Reliability Baseline
Pedagogical Alignment
Content and Data Integrity
Safety and Cyber-Resilience

a. The first baseline requirement for reliable public EdAI is pedagogical alignment, designed to prevent cognitive offloading, where systems can raise short-term task performance without commensurate learning gains.[37] The educational significance of EdAI will be realised through specific and informed digital pedagogy, including adaptive and personalised learning, and learner engagement and motivation.[38] Pedagogy-aligned reliability should therefore be operationalised as a minimum baseline in three ways. *First, NETF* should define interaction rules for learner-facing tools, specifying when full solutions are allowed and when scaffolded prompting and reflection are required. *Second*, NETF should define standard metrics and evaluation artefacts that test learning transfer under real-time use conditions.[39] *Third*, governance should require continuous monitoring against these learning-outcome indicators, ensuring deployment anchored in demonstrable and durable learning outcomes rather than engagement proxies. A useful analogue is the UK Department for Education's AI product safety expectations for learner-facing tools, which emphasise monitoring and reporting requirements associated with cognitive offloading and usage intensity (for e.g., expects tools to provide data on: (a) the rate of requests for cognitive offloading and the amount of cognitive offloading delivered, (b) each learner's duration of usage, and (c) a measure of personal/emotional engagement (captured as the nature of information exchanged, without disclosing the content)), as well as teacher-mediated controls for higher-risk learner modes (for e.g., where full solutions are readily available).[40] Similarly, the OECD emphasises purpose-built design, stakeholder co-creation, and rigorous trials to support institutional trust and safer procurement, with greater emphasis on pre-deployment testing than post-deployment remediation for EdAI.[41]

[35] Jafar, K., Ananthpur, K., & Venkatachalam, L. (2023). Digital divide and access to online education: New evidence from Tamil Nadu, India. *Journal of Social and Economic Development*, https://doi.org/10.1007/s40847-023-00236-1; PIB, Ministry of Finance, Government of India (2025). India's school education system, Economic Survey 2024–25. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2097864&reg=3&lang accessed January 2026

[36] Source: Authors

[37] OECD Digital Education Outlook 2026: Exploring Effective Uses of Generative AI in Education https://doi.org/10.1787/062a7394-en accessed January 2026

[38] Foster, D., McLemore, C., Olszewski, B., Chaudhry, A., Cooper, E., Forcier, L., & Luckin, R. (2023, December). *EdTech Quality Frameworks and Standards Review: DfE Quality Characteristics Project (ref: PQFFSR).* Department for Education. https://assets.publishing.service.gov.uk/media/6579d0ac0467eb001355f761/EdTech_quality_frameworks_and_standards_review.pdf accessed January 2026

[39] This must include performance without tool access and delayed retention. UNESCO. (2023). Guidance for generative AI in education and research. UNESCO. https://doi.org/10.54675/EWZM9535; Department for Education. (2025, August 12). Generative artificial intelligence (AI) in education (Policy paper) https://www.gov.uk/government/publications/generative-artificial-intelligence-in-education/generative-artificial-intelligence-ai-in-education; Brown, C. L., Kaur, S., Kingdon, G., & Schofield, H. (2022, June). Cognitive endurance as human capital (Working Paper No. 2022-73). Becker Friedman Institute for Economics, University of Chicago. https://thedocs.worldbank.org/en/doc/2b9849ff027d18718c7092be6b1887be-0050022025/original/Cognitive-Endurance-as-Human-Capital.pdf Buildng the ability to sustain performance over time during a cognitively effortful task (i.e., keep thinking when it's hard, not outsource the hard parts) accessed January 2026

[40] Department for Education. (2025, January 22). *Generative AI: Product safety standards.* (Last updated January 19, 2026). https://www.gov.uk/government/publications/generative-ai-product-safety-standards/generative-ai-product-safety-standards It also expects friction or teacher approval before switching into modes where full solutions are readily available, and requires products to track and report offloading.(for e.g., clicking to reveal full solutions, pasting text instead of writing, accepting near-complete autocomplete, or using "complete this for me" options).

[41] Finally, we alos interpret a pedagogy-aligned reliability can be strengthened through baseline disclosure norms for example, requiring learners to

b. Educational content governance is often provider-defined and implemented through a set of rules: policy, standards, curricula mapping, model tuning, prompt constraints, input/output filtering or parsing, and retrieval workflows that collectively shape model behaviors and outputs. Specifically, UNESCO advances performance measurement as use-case specific: while "accuracy" may capture how often a tool produces correct answers in mathematics, in open-ended or subjective contexts a key indicator may instead be "answer rate" (how often the system answers directly rather than refusing or deferring).[42] However, because models are opaque and update-sensitive, these controls are an unstable basis for education assurance unless complemented by certain quality assurance duties across the model lifecycle. Accordingly, NETF should specify, at minimum: *First*, provenance and labelling requirements for both AI-generated and original learning assets, including traceable sources for retrieval corpora, question banks, and other content stores, documented in consistent formats; and *second*, continuous assurance requirements across the model lifecycle, including drift and degradation monitoring, structured human evaluation, versioning and change logs, and mandatory revalidation (or benchmarked regression testing) after any material updates to the model, prompts, tools, or underlying corpora.[43] These duties must also apply to AI-assisted evaluation, where opacity, bias, and inconsistency can directly harm learners through unfair or unstable assessment outcomes.

c. Public EdAI deployments operate in a high-threat environment, and failures can arise not only from model error but also from adversarial manipulation, credential compromise, unsafe integrations, or data exposure. Security and cyber resilience components must therefore be treated as a baseline for reliability. The NETF should specify adversarial-testing and incident-readiness requirements (prompt-injection/jailbreak resistance, least-privilege access, logging, containment procedures, clear escalation and response playbooks) for EdAI and require cyber-safety for public deployments. A useful analogue is the UK Department for Education's core digital and technology standards for schools and colleges, including dedicated expectations for cyber-resilience, filtering and monitoring, documented reviews, defined responsibilities, and escalation procedures.[44] Within India's context, these controls should be integrated into EdAI deployment guidance and participation requirements so that security-resilience is embedded at the point of procurement, integration, and continuous operation.

Collectively, these baseline duties define ***reliability*** for public EdAI as learning-appropriate behavior, dependable content and evaluation integrity over time, and secure, resilient operation. Without a minimum baseline, small errors and vulnerabilities can scale rapidly across diverse classrooms and persist through successive cohorts of models and content pipelines, undermining learning outcomes and institutional trust.

indicate whether, and how, AI tools were used in homework thereby informing institutional decision-making understanding of AI's impacts on learning behaviours and outcomes over time. Global reference model used: OECD's "purpose-built and co-created and rigorously trialled" framing for trustworthy adoption, UK DfE's product-safety expectations/standards (including reliable harmful-content prevention and reliability as a security-adjacent technical objective), EU AI Act Annex III sensitivity signals for education uses, NIST's GenAI risk-management profile (lifecycle governance for poisoning/prompt-injection-type risks), and TEAS's deployment-readiness pillars (verifiability, stability, auditability, pedagogical soundness) accessed January 2026

[42] UNESCO, Guidance for generative AI in education and research. UNESCO. https://doi.org/10.54675/EWZM9535 accessed January 2026

[43] NIST's GenAI risk profile explicitly flags the *cadence of vendor releases and updates* as a governance factor and calls for content-provenance processes (documenting the origin of training and generated data) and periodic review to address unexpected changes

[44] Association of Network Managers in Education (ANME). (2025, November 17). IT support standards [PDF]. (Prepared from information from the Department for Education.) https://files.anme.co.uk/dfe/DfE%20IT%20Support%20Standards.pdf accessed January 2026 (covering six core standards: Broadband internet, Cyber security, Digital leadership and governance, Filtering and monitoring, Network switching, Wireless network); Department for Education. (2026, February 2). Filtering and monitoring: Core standard (Meeting digital and technology standards in schools and colleges) https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-core-standard accessed January 2026

CHAPTER 2:

Trust and Safety Benchmarks for Defence Technology LLMs

Introduction

Across multiple use-cases, there has been a significant rise of Generative AI ("**GenAI**") based systems in defence applications. The central characteristic of GenAI to learn patterns and generate output from text, benefits multiple applications of defence technology ("**DefTech**"), like supply chain and logistics management, battle simulation, and adaptive threat hunting.[45] Many militaries have, accordingly, strategized and implemented AI plans for military applications across wartime and peace-time operations.[46]

These action plans target principles of implementation, mitigation strategies, and safety mechanisms to prevent risks accruing from AI. With GenAI systems specifically, the problems of model architecture can potentially pose risks in such a high intensity use case. Defence use cases are traditionally high risk, using sensitive data, and can translate to risks to human life. GenAI traditionally poses the risk of hallucination, model drift, and biased output. In addition to traditional cybersecurity risks to technical architecture, GenAI use creates more external cybersecurity risks like prompt injection, data exfiltration, or model poisoning, which makes AI applications in defence particularly prone to adversarial attacks by those seeking to destabilize them.

In framing a response, it is important to account for the risks from model architecture while selecting base models for specific defence applications. Benchmarking for specific risks allows downstream model developers to pick the most suitable model for their applications.

Regulatory Impetus for Trusted and Safe Systems for DefTech Applications

India has developed a multi-layered framework to regulate generative AI within its defence sector, combining overarching national AI governance principles with defence-specific cybersecurity and procurement protocols. At the national level, India's AI Governance Guidelines (2025), issued by MeitY, establish seven guiding principles for AI development. These cross-sectoral principles apply to governing AI applications in defence. Relatedly, for specific sectoral applications, the Defence Acquisition Procedure ("**DAP 2020**") requires Headquarters Integrated Defence Staff ("**HQ IDS**") to examine possibilities for including AI in defence platforms and systems, while classifying AI as a field with "significant national security implications". A new Draft Defence Acquisition Procedure, 2026, is being circulated for public comments in February, 2026. The draft does not intend to explicitly introduce novel AI-focused trust and safety requirements. Considering its status as draft law, a discussion on the substantive and acquisition related aspects of the new procedure are beyond the scope of this essay.

These structures for AI governance are accompanied by robust cybersecurity and data protection requirements. The Cyber Security Policy, 2019 by the Ministry of Defence mandates Chief Information Security Officer ("**CISO**") appointments, Cyber Security Groups and Cells for cyber governance, CERT-In coordination, air-gap policies, and continuous user training for all defence entities. Similarly, the Security Manual for Licensed Defence Industries significantly expands cybersecurity requirements for licensed defence contractors, mandating intrusion detection systems, air-gapped networks, and integration with the MoD's Cyber Security Operations Centre ("**CSOC**") for real-time monitoring, while also requiring secure configuration protocols for AI systems. Moreover, for AI and cloud services, data localization is mandatory. AI services must be delivered through Indian data centers, and user data cannot be transferred outside India.

Many of the structural regulations to ensure safe AI are derived from mandatory contractual clauses that ensure supply chain integrity. However, many of these obligations focus heavily on cybersecurity, over other principles of trustworthiness and resilience of the AI system itself. Trustworthiness of the system relies both on the ability of the user to rely on the output being generated, which requires accuracy and lack of bias, as well as the reliability of the data being used to train the model. Safety requires the system to not have unintended harms in its use, which also includes dimensions like accuracy. It also means that systems need to be thoroughly audited for legal risks.

[45] Aditya K Sood, "Revolutionizing Cyber Defense: Leveraging Generative AI for Adaptive Threat Hunting" (2025) 8 Internet Technology Letters.

[46] Department of Defence, USA, "Summary of the 2018 Department of Defense Artificial Intelligence Strategy" (DoD, USA, 2018) https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF accessed November 12, 2025.

Other jurisdictions have emphasized the need for Responsible AI governance structures while applying AI to defence use cases. The US DoD's Responsible Artificial Intelligence Strategy and Implementation Pathway highlight continuous oversight, risk assessment from project outset, mitigation of unintended consequences, and justified confidence in AI systems. The UK MOD's Defence Artificial Intelligence Strategy also highlights the requirement for continuous testing, evaluation, verification and validation ("**TEV&V**"). These evaluations focus on live testing across the AI lifecycle, to provide a more holistic view of risks accruing from AI use. India's regulatory response seemingly lacks this nuance, leaving it prone to AI risk manifestation.

This also means that the internal model is not being vetted for risks manifesting from the architecture. Trust and safety assessments, which look at the reliability of the model, are accordingly important for ascertaining the usability of a particular model, especially in defence use cases. While cybersecurity is an important facet in defence, model architecture may itself lead to risks which are not external. Trust and safety evaluations usefully solve such concerns.

Implementing Trust and Safety Vectors in Defence Tech Applications

Risks in GenAI and Defence Applications

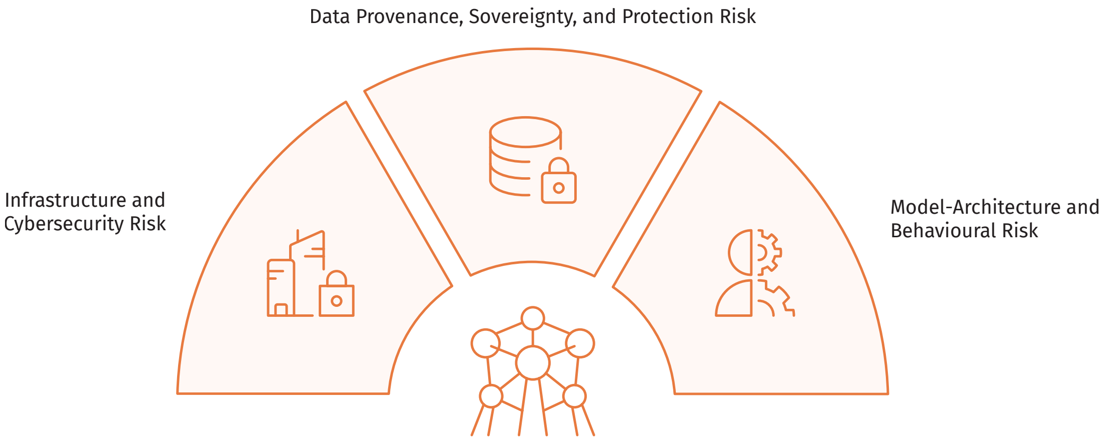
Risks emanating from downstream applications of GenAI are threefold; there are infrastructural and cybersecurity risks, there are data provenance and protection risks, and there are risks that emanate from the model architecture that can be magnified in certain sensitive use-cases. (*Refer Illustration 5*)

Processing data at large scale requires investment in significant hardware and software infrastructure. Military data and documents are especially high risk, since they are classified, and thus security of infrastructure is of immense concern. The risk stemming from hardware is further exacerbated when cloud systems are used to store and process data.[47] Cloud systems may not necessarily be stored internally. Even with data localisation, other facets of the application may be external, leading to migration risks associated in this case.

Data is integral to the functioning of AI systems, and DefTech relies on accurate and updated information that is fed to AI and ML systems. However, accessing and using large amounts of data comes with significant risks. When DefTech is outsourced to private technology companies, it risks shifting critical data from the public sector to the private sector.[48] This in turn can vex data sovereignty. Technology providers traditionally have a global reach, as opposed to the needs of domestic defence ministries. Not having control over the data collected by private parties can lead to erosion of domestic sovereignty over critical data and increased dependence on the party for executive defence-sensitive functions.[49] Connectedly, excessive data collection of sensitive personal data can also cause legal and ethical harm, especially if the data collected is disproportionate, and can lead to bias.

AI models and generative AI present distinct risks in defence contexts that extend beyond traditional software vulnerabilities. Hallucinations represent a critical concern, as large language models can generate plausible but entirely fabricated intelligence assessments, operational details, or threat analyses that could mislead commanders. Model opacity compounds these risks, as defence operators often

Illustration 5: GenAI Risk Structure in Defence Applications


Data Provenance, Sovereignty, and Protection Risk
Infrastructure and Cybersecurity Risk
Model-Architecture and Behavioural Risk

[47] IBM, U.S. Army Selects IBM for the Third Time to Provide Full Portfolio of IT Management Services (*IBM*, February 10, 2021) https://newsroom.ibm.com/2021-02-10-U-S-Army-Selects-IBM-for-the-Third-Time-to-Provide-Full-Portfolio-of-IT-Management-Services accessed November 12, 2025.

[48] Springer Nature, Ethical, legal, and social challenges of data economy in defence the case of battlefield data https://link.springer.com/article/10.1007/s00146-025-02610-5 accessed Jan 2026

[49] The Guardian, Elon Musk ordered Starlink to be turned off during Ukraine offensive, book says https://www.theguardian.com/technology/2023/sep/07/elon-musk-ordered-starlink-turned-off-ukraine-offensive-biography

cannot understand why a foundation model produced outputs, undermining accountability and trust. Additionally, over-reliance on AI-generated content may cause automation bias, where operators uncritically accept machine outputs and fail to apply necessary human judgment in life-or-death decisions. Reports indicate that AI technologies leveraged during the Israel-Hamas conflict incorrectly classified combatants at an approximate error rate of 10%.[50] Such misclassification in both conflict and non-conflict use cases diminishes the efficacy of the AI system and potentially causes significant harm.

In developing the risk axes relevant to defence AI, several critical dimensions emerge. Bias and discrimination represent a central concern, as AI systems can produce systematically biased outputs affecting target identification, threat assessment, or resource allocation, potentially creating discriminatory outcomes against specific populations. Bias can manifest as a data provenance risk, where training datasets over-represent or under-represent certain categories of data, or as a model risk, wherein GenAI systems incorrectly reason and categorize outputs due to irrelevant factors, more commonly known as the black-box problem. Transparency failures, characterized by insufficient disclosures regarding data provenance and decision-making processes, undermine accountability in ways that are particularly problematic in defence contexts where legal responsibility must be clearly established. These sites of risks can potentially translate to a lack of trust in AI generated outputs for the DefTech sector. Clear lines of accountability need to be made to ensure that AI systems can be integrated fully into the defence ecosystem. While cybersecurity and guarding against external threats is of key importance, integration of trust and safety mechanisms should also happen coterminously to ensure development of the DefTech sector without major impediments.

Key principles for developing benchmarking metrics and evaluating DefTech risks

AI integration in defence operations presents unique challenges for trust, safety, bias mitigation, and fairness, requiring rigorous benchmarking frameworks that differ significantly from commercial applications. The defence context demands evaluation methods that account for high-stakes decision-making, adversarial conditions, and compliance with international humanitarian law.

Specifically, for trust and safety, benchmarks can help identify potential points of failure in AI integration. Current benchmarks focus inadvertently on general-purpose AI and harms that arise from these applications.[51] However, more specifically targeted defence benchmarks can highlight more domain concerns, especially with bias and resilience.

From our risk analysis, a few categories emerge as the sites for creating targeted benchmarks that are tailored to defence applications. Table 2.1 contains the relevant areas which will need to be considered while creating benchmarks for defence applications. The sites of research are the areas from which the relevance of the benchmark occurs. These are mapped onto relevant principles that should be operationalized in any given DefTech application. The categories of metrics then analyse what kind of metrics can be distilled, and those form the crux on which the benchmark suite should be created.

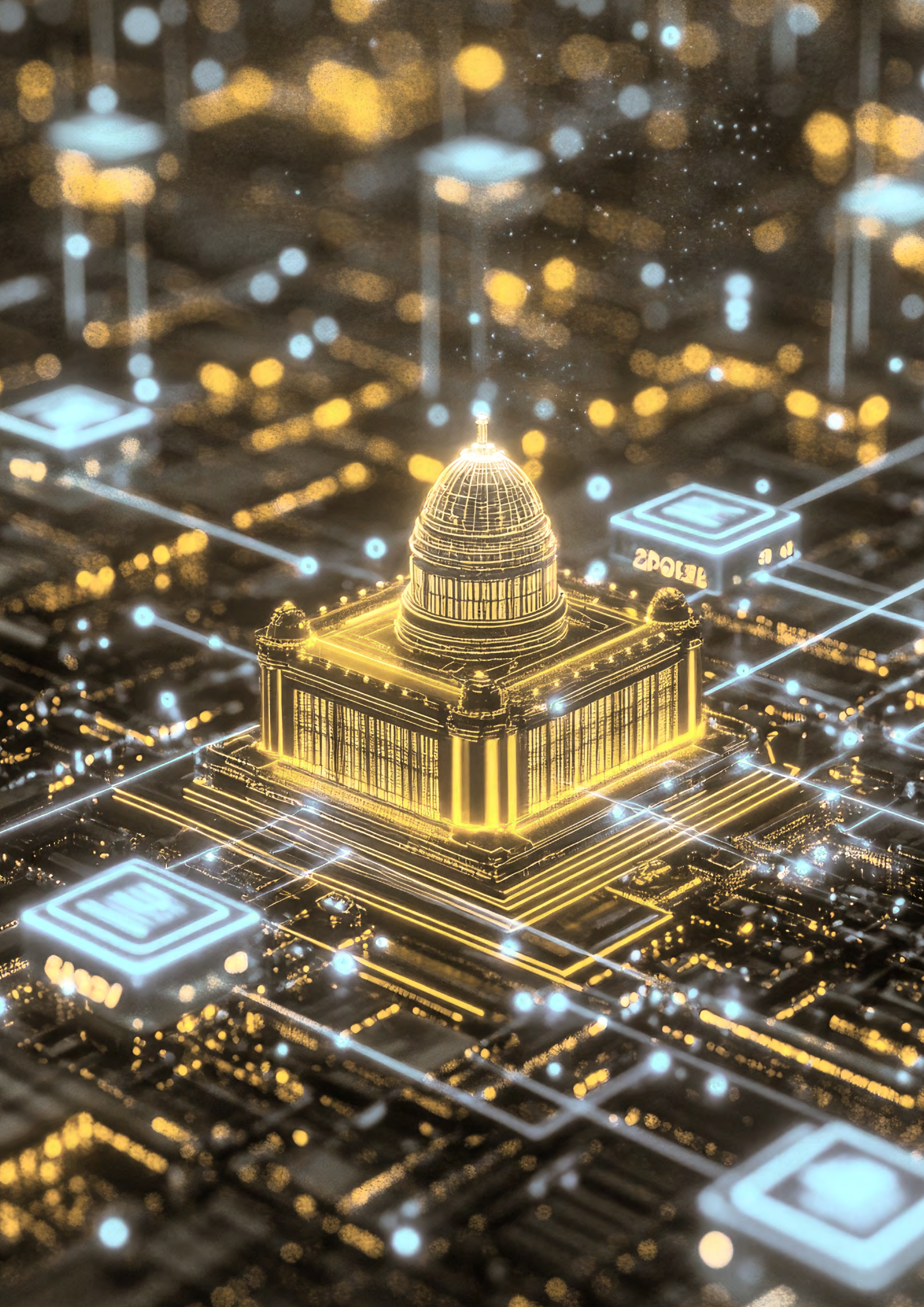
Table 2.1

Sites of research	Principles that underlie implementation	Categories of metrics
International Humanitarian Law and other relevant jurisprudence	Legality of actions, accountability, sovereignty, and human rights	Adherence to relevant laws, bias in outputs
Municipal laws (including data privacy, legality of AI use, criminal law, etc)	Data provenance and protection, legality	Adherence to relevant laws
Trust and safety principles for AI use	Sovereignty of data, reliability of AI systems	Accuracy, Bias and fairness

Robust benchmarking addresses defence AI risks through multiple mechanisms. Without credible benchmarking, defence AI adoption risks becoming a faith-based enterprise where leaders cannot make informed trade-offs between automation and human judgment, making the establishment of rigorous evaluation frameworks essential for responsible military AI integration. Although benchmarking can help form a sound understanding of the limitations of models for use in defence purposes, it cannot substitute for full red-teaming and legal risk diligence of the final application. Issues with overfitting will remain when benchmarks are used to evaluate output in the training stage. A response to this risk is, however, beyond the domain of this essay.

[50] Tara John, Israel Is Using Artificial Intelligence to Help Pick Bombing Targets in Gaza, Report Says (CNN, April 3, 2024), “https://edition.cnn.com/2024/04/03/middleeast/israel-gaza-artificial-intelligence-bombing-intl“; ”https://edition.cnn.com/2024/04/03/middleeast/israel-gaza-artificial-intelligence-bombing-intl accessed Jan 2026

[51] See generally; IndicBias, a benchmark for measuring bias in Indian contexts for LLMs (https://arxiv.org/pdf/2403.20147); Truthful QA, a benchmark for testing prompts on generated falsehoods (https://arxiv.org/pdf/2109.07958) accessed 2026



CHAPTER 3:

Joint Parliamentary Committee as an Instrument for AI Governance

Background

India has been quick to adopt AI-driven innovation, but does not have a comprehensive framework to govern Artificial Intelligence (**'AI'**). While efforts have been made to introduce a Private Member's Bill on AI, the Bill did not receive legislative assent.[52] Even if the said Bill were to have seen the light of the day, the broad and undefined scope of what counts as AI and the lack of a risk-based tiering framework would have failed to provide clear criteria to differentiate low-risk from high-impact systems or carve out associated obligations proportionately.

Currently, India derives its AI regime from a host of Acts, Rules, advisories, national strategies, principles and sector-specific regulations.[53] Such a piecemeal and reactive approach to AI regulation—relying on existing laws and non-binding guidelines—has been criticized and raises concerns for being inadequate, creating regulatory uncertainty, and failing to address specific risks such as algorithmic bias, model drift or deepfakes. Given this, a thorough review of the AI regime is the need of the hour. In such a scenario, the onus falls upon the Parliament – the apex lawmaking institution – to step in and curate a framework that inspires trust and facilitates growth.

This then begs the question as to how we approach lawmaking on AI in India. Effective lawmaking on any subject, more particularly AI, cannot be achieved unless our lawmakers make the best possible use of the legislative instruments to determine and develop a robust solution to the challenges presented by an AI-driven world. This essay unpacks the optimal pathway to leverage legislative processes to optimally govern AI.

Assessment of the Current Legislative Approach

Pathways to Legislative Deliberation on AI

A detailed assessment of the AI framework by a parliamentary committee can be valuable. These committees, established under the Indian Constitution,[54] act as a "mini parliament" that provides the opportunity to delve deeper into matters of public concern and develop expert opinions. The parliamentary committees can either be Departmentally Related Standing Committees (**'DRSC'**), which are permanent committees that examine Bills related to specific ministries and invite public comments and expert opinions, or Select or Joint Committees, which are temporary or *ad hoc* committees formed to examine a particular Bill on a clause-by-clause basis.

Apart from the assessment by committees or the direct passage of a Bill, the Rules of Procedure and Conduct of Business in Lok Sabha (**'Lok Sabha Rules'**) and the Rules of Procedure and Conduct of Business in Rajya Sabha (**'Rajya Sabha Rules'**) provide for other deliberative motions and devices to encourage discussion on legal matters. These include the Question Hour,[55] Zero Hour,[56] Calling Attention Motion,[57] Short Duration Discussion[58] and Half-

[52] The Artificial Intelligence (Ethics and Accountability) Act, 2025 was introduced by Smt. Bharti Paridhi on January 20, 2025 in the Lok Sabha. *See* https://sansad.in/getFile/BillsTexts/LSBillTexts/Asintroduced/59%20of%202025%20AS125202594603PM.pdf?source=legislation accessed 2026

[53] India's key AI-related regulation is embedded in the following frameworks: The Digital Personal Data Protection Act, 2023, IT (Intermediary Guidelines & Digital Media Ethics Code) Rules, 2021 MeitY's India AI Governance Guidelines (2025) and Advisory dated 01.03.2024, NITI Aayog's National Strategy for AI (2018) and Principles for Responsible AI (2021), and sectoral regulations like the Framework for Responsible and Ethical Enablement of Artificial Intelligence (FREE-AI).

[54] Article 118 of the Indian Constitution empowers each House of Parliament (i.e. the Lok Sabha and the Rajya Sabha) to create its own rules for procedure and business conduct.

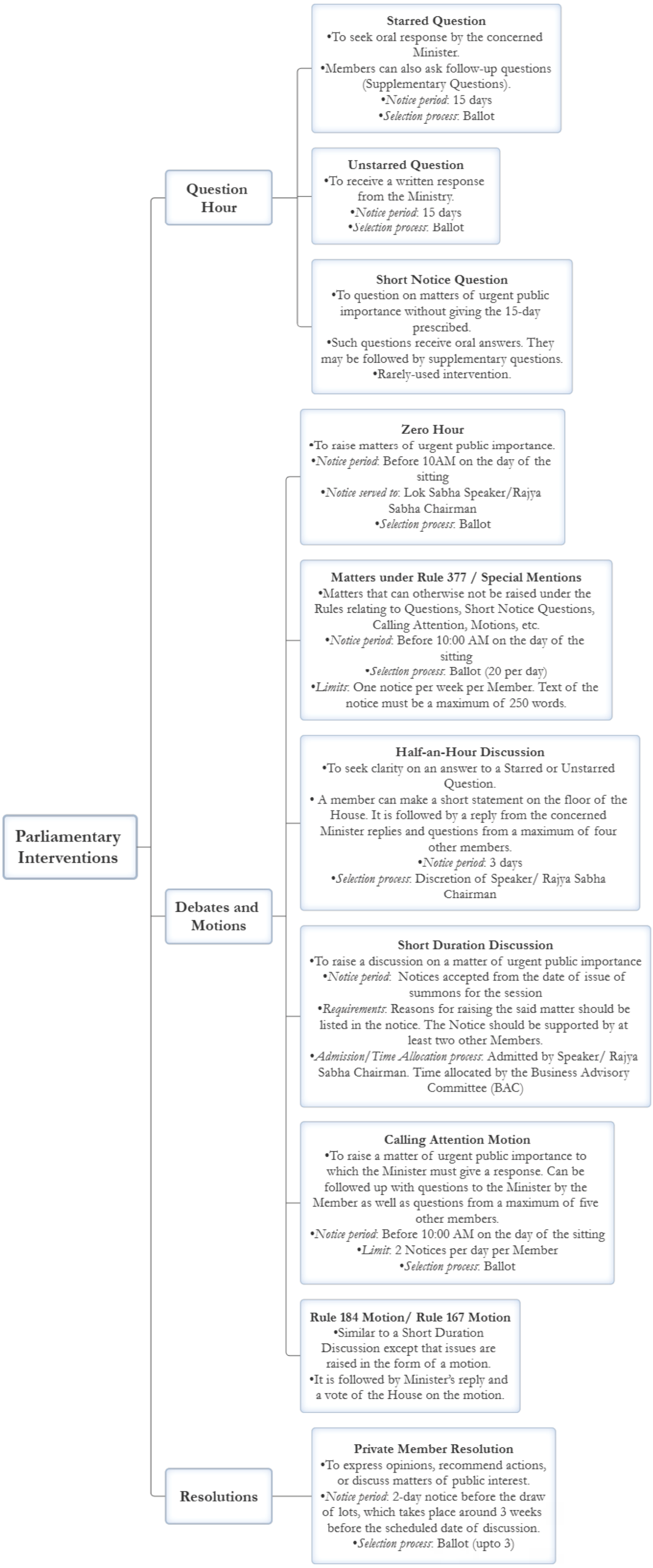
[55] Rules 41-44, Lok Sabha Rules https://sansad.in/uploads/Rules_of_Procedures_E_9d8fd0f4c3.pdf?updated_at=2022 - and Rules 47-50, Rajya Sabha Rules https://cms.rajyasabha.nic.in/UploadedFiles/LegislativeSection/LegislativeRules/English_2052022english_3092021rules_pro.pdf.

[56] A Zero Hour is a parliamentary innovation of India which has not been specified under the official Rules of Procedure of the Houses. It commences at around 12 PM, following the Question Hour, and allows Members to raise urgent matters of public importance.

[57] Rules 197, Lok Sabha Rules and Rule 180, Rajya Sabha Rules.

[58] Rules 193, Lok Sabha Rules and Rule 176, Rajya Sabha Rules.

Illustration 6 - Parlimentary Interventions



Parliamentary Interventions

Question Hour

Starred Question
•To seek oral response by the concerned Minister.
•Members can also ask follow-up questions (Supplementary Questions).
•*Notice period*: 15 days
•*Selection process*: Ballot

Unstarred Question
•To receive a written response from the Ministry.
•*Notice period*: 15 days
•*Selection process*: Ballot

Short Notice Question
•To question on matters of urgent public importance without giving the 15-day prescribed.
•Such questions receive oral answers. They may be followed by supplementary questions.
•Rarely-used intervention.

Debates and Motions

Zero Hour
•To raise matters of urgent public importance.
•*Notice period*: Before 10AM on the day of the sitting
•*Notice served to*: Lok Sabha Speaker/Rajya Sabha Chairman
•*Selection process*: Ballot

Matters under Rule 377 / Special Mentions
•Matters that can otherwise not be raised under the Rules relating to Questions, Short Notice Questions, Calling Attention, Motions, etc.
•*Notice period*: Before 10:00 AM on the day of the sitting
•*Selection process*: Ballot (20 per day)
•*Limits*: One notice per week per Member. Text of the notice must be a maximum of 250 words.

Half-an-Hour Discussion
•To seek clarity on an answer to a Starred or Unstarred Question.
• A member can make a short statement on the floor of the House. It is followed by a reply from the concerned Minister replies and questions from a maximum of four other members.
•*Notice period*: 3 days
•*Selection process*: Discretion of Speaker/ Rajya Sabha Chairman

Short Duration Discussion
•To raise a discussion on a matter of urgent public importance
•*Notice period*: Notices accepted from the date of issue of summons for the session
•*Requirements*: Reasons for raising the said matter should be listed in the notice. The Notice should be supported by at least two other Members.
•*Admission/Time Allocation process*: Admitted by Speaker/ Rajya Sabha Chairman. Time allocated by the Business Advisory Committee (BAC)

Calling Attention Motion
•To raise a matter of urgent public importance to which the Minister must give a response. Can be followed up with questions to the Minister by the Member as well as questions from a maximum of five other members.
•*Notice period*: Before 10:00 AM on the day of the sitting
•*Limit*: 2 Notices per day per Member
•*Selection process*: Ballot

Rule 184 Motion/ Rule 167 Motion
•Similar to a Short Duration Discussion except that issues are raised in the form of a motion.
•It is followed by Minister's reply and a vote of the House on the motion.

Resolutions

Private Member Resolution
•To express opinions, recommend actions, or discuss matters of public interest.
•*Notice period*: 2-day notice before the draw of lots, which takes place around 3 weeks before the scheduled date of discussion.
•*Selection process*: Ballot (upto 3)

an-Hour Discussion.[59] Here too, there has been inadequate utilisation of the legislative instruments available to our elected representatives.

Figure: Parliamentary Interventions that can be utilised by Members of Parliament to facilitate engagement and discussion on AI.[60]

For instance, a Member of Parliament (**'Member'**) can bring a specific urgent matter to the attention of a Minister through a Calling Attention Motion, prompting an authoritative brief statement from the concerned Minister.[61] Similarly, a Member can facilitate a discussion up to two and a half hours on urgent public issues that require immediate attention through a Short Duration Discussion. This discussion culminates into a response from the concerned Minister without a formal motion or vote.[62] We are yet to witness dedicated debates on AI as part of these parliamentary interventions.

Alternatively, a Rule 377 intervention under the Lok Sabha Rules allows Members to raise matters of urgent public importance that do not fall under the purview of standard, formal proceedings, such as motions or questions. The Lok Sabha records show that there has been merely one intervention related to AI under Matters under Rule 377 during the eighteenth Lok Sabha.[63] The Rajya Sabha Rules provide for a similar mechanism known as "Special Mentions" under Rule 180A-E.

Legislators and AI

The Indian Parliament itself is actively using AI for translating business documents, analysing debates, and transcribing across 22 languages. A dedicated "Parliamentary Language Dictionary" comprising 48,000 terms has also been developed which has been integrated into a custom AI model for exclusive parliamentary use. Further, the Deputy Chairman of the Rajya Sabha[64] recently called for synergy between the Parliament and State Legislatures for efficient adoption on AI, and highlighted the need for a 'Data Lake' where the collective knowledge on legislative debates across the country can be used to train the models best suited for the Indian context.[65]

The Committee discussions on AI so far have been undertaken by multiple entities. The Ministry of Electronics and Information Technology ("**MeitY**") formed four committees in 2019 to shape India's AI strategy across various sectors.[66] Another committee, the "Subcommittee on AI Governance and Guidelines Development", was set up in 2023, which was tasked with reviewing existing global laws and analysing literature on AI and whose report informed the India AI Governance Guidelines released in 2025.[67] The Standing Committees, such as the one on Home Affairs or Defence, are also actively reviewing AI integration which may lead to inconsistent and conflicting outcomes.

Newer committees have been set up to review other AI-driven disruptions. Recently, during her 2026 Budget Speech, the Finance Minister[68] announced the setting up of a Standing Committee on "Education to Employment and Enterprise" to review the impact of AI on India's services sector.[69] However, the constraint is that this panel shall recommend measures in the context of the services sector alone, as opposed to assessing the holistic approach towards curating an effective AI regime. A subject as vital and all-encompassing as AI deserves a more dedicated approach.

[59] Rules 55, Lok Sabha Rules and Rule 60(2), Rajya Sabha Rules.

[60] Source: Author

[61] Rajya Sabha, calling attention https://cms.rajyasabha.nic.in/uploadedfiles/procedure/practiceandprocedure/english/8/calling_attention.pdf accessed January 2026

[62] Rajya Sabha, Motions, Resolutions And Short Duration Discussion, https://Cms.Rajyasabha.Nic.In/Uploadedfiles/Procedure/Practiceandprocedure/English/7/Motion_resolution.Pdf accessed January 2026

[63] Rajya Sabha, Motions, Resolutions And Short Duration Discussion, https://cms.rajyasabha.nic.in/UploadedFiles/Procedure/PracticeAndProcedure/English/7/motion_resolution.pdf Rajya Sabha, Point of Order, https://sansad.in/uploads/20_POINTS_OF_ORDER_point_order_31ada04381.pdf "*Raising a matter which is not a point of order. A member who wishes to bring to the notice of the House a matter which is not a point order, shall give notice in writing to the Secretary General specifying clearly and precisely the text of the matter to be raised. The member shall be permitted to raise it only after the Speaker has given the consent and at such time and date as the Speaker may fix.*" PIB, India AI Governance Guidelines, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2228315&reg=3&lang=2 accessed January 2026

[64] PIB, Institutional knowledge of humans central to developing accountable AI for Parliaments: Deputy Chairman Shri Harivansh, https://www.pib.gov.in/PressReleseDetail.aspx?PRID=2214979&reg=3&lang=1 Shri Harivansh Narayan Singh

[65] GOI, PIB, Deputy Chairman, Rajya Sabha, Shri Harivansh calls for *synergy between Parliament and State Legislatures for efficient adoption of AI* https://www.pib.gov.in/PressReleasePage.aspx?PRID=2216450&reg=3&lang=1#:~:text=Underlining%20a%20vision%20for%20harmonious,Parliamentary%20knowledge%20is%20unique accessed January 2026

[66] MEITY, Artificial Intelligence Committees Reports , https://www.meity.gov.in/documents/reports/report-of-committee-gN0YTNtQWa?pageTitle=Artificial-Intelligence-Committees-Reports-(2019) accessed January 2026

[67] MEITY, Report on AI Governance Guidelines Development ,https://www.meity.gov.in/content/report-ai-governance-guidelines-development-public-consultation accessed January 2026

[68] Smt. Nirmala Sitharaman

[69] PIB, Union Education Minister Lauds Historic Budget 2026-27, Calling It A Yuva Shakti Driven https://www.pib.gov.in/PressReleasePage.aspx?PRID=2221734&reg=3&lang=1 accessed January 2026

The Way Forward

Bridging the gap between our present framework and a secure, trustworthy AI-regime requires concerted efforts towards capacity-building programs for policymakers, active collaboration and partnerships with industry and academia, and meaningful institutional reforms to lend crucial advisory and research support towards rulemaking.

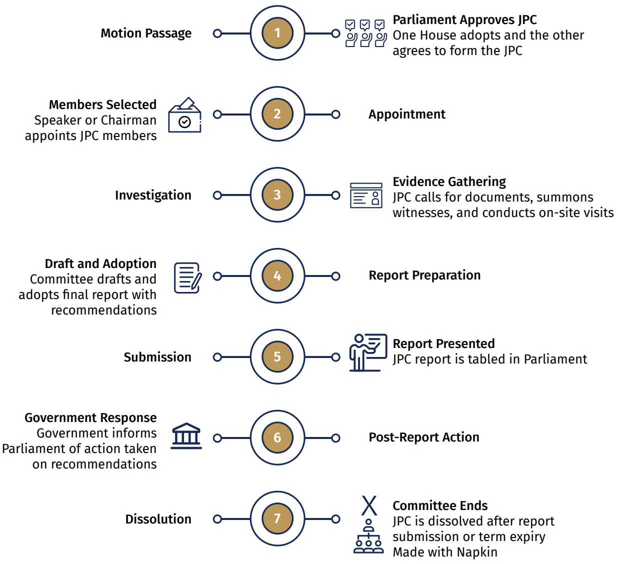
The Inter-Parliamentary Union, for instance, has released Guidelines on developing AI literacy. These Guidelines acknowledge the need for a well-trained parliamentary workforce and better-informed parliamentarians as it will allow them to make reasoned choices about the adoption of AI technology, curate and shape appropriate laws and regulations, and effectively oversee AI-driven initiatives.[70] India can borrow from the structure proposed by these Guidelines to implement the AI literacy programmes for its lawmakers and parliamentary staff. However, while we must strive to educate our lawmakers and strengthen the parliamentary ecosystem from within, such changes take time to take effect and cannot be relied upon as a sole measure to achieve tangible outcomes. The challenges presented by AI must be tackled with a more action-oriented lawmaking approach.

The MeitY has recently indicated that the government is not inclined towards bringing in new laws or regulations on AI unless it is "absolutely necessary".[71] Instead, it seeks to utilise the existing laws, like the Information Technology Act, 2000 (**'IT Act'**) and the Digital Personal Data Protection Act, 2023 (**'DPDP Act'**), to address AI-related issues. While the government may intend to be mindful in its approach to ensure that it does not hinder innovation in the technology sector, the idea as to whether India's current approach is adequate or whether it needs a standalone AI legislation needs deeper scrutiny.

In a day and age where leading jurisdictions, such as the European Union (**'EU'**), have enacted a dedicated AI law[72], or are in the process of working on a draft law[73], such as Brazil, the need for a comprehensive AI-regime cannot be negated. Alternatively, India could benefit from a fast-tracked, sector-specific approach,[74] such as the one deployed by China,[75] that collectively functions as a comprehensive, centralized regulatory regime.

This is where the role and function of a Joint Parliamentary Committee (**'JPC'**) becomes paramount. A JPC is a legislative tool designed to investigate specific bills or scrutinize complex subject matters involved in legislation. It acts as an oversight mechanism by holding the government accountable for its actions and policies. Being *ad hoc* and multipartisan in nature, it facilitates reduction of bias in investigating sensitive issues having large-scale impact.

Illustration 7 - Stages of a Joint Parliamentary Committee (JPC)


Motion Passage
1
Parliament Approves JPC
One House adopts and the other agrees to form the JPC
Members Selected
Speaker or Chairman appoints JPC members
2
Appointment
Investigation
3
Evidence Gathering
JPC calls for documents, summons witnesses, and conducts on-site visits
Draft and Adoption
Committee drafts and adopts final report with recommendations
4
Report Preparation
Submission
5
Report Presented
JPC report is tabled in Parliament
Government Response
Government informs Parliament of action taken on recommendations
6
Post-Report Action
Dissolution
7
Committee Ends
JPC is dissolved after report submission or term expiry
Made with Napkin

(*Refer Illustration 7*): Stages of a JPC: from Constitution to Dissolution.[76]

[70] Inter Parliamentary union, *Training for Data Literacy and AI Literacy*, https://www.ipu.org/ai-guidelines/training-data-literacy-and-ai-literacy-developing-ai-literacy accessed January 2026

[71] *See* The Week, Govt prefers existing laws over new regulations to govern AI focus on innovation Meity Secy, "https://www.theweek.in/wire-updates/business/2025/12/16/dcm25-biz-meity-ai-regulations.html accessed January 2026; *As it is, we are a country with many laws…So my own inclination always is to avoid putting in a new law, a new regulation, unless you absolutely have to. Try to see what we can do with existing law.…Our approach to regulation of AI thus far has been very, very grounded and has been very, very clear that under no circumstances do we want to get in the way of innovation."*

[72] EU AI Act

[73] Bill No. 2,338/2023 (PL 2338/2023), often referred to as the Brazilian AI Act or Legal Framework for Artificial Intelligence., https://artificialintelligenceact.com/brazil-ai-act/.

[74] Binding Hook, *China's generative AI boom isn't just technological*, https://bindinghook.com/chinas-generative-ai-boom-isnt-just-technological-its-regulatory/ accessed January 2026

[75] Key Regulations include the Interim Measures for the Management of Generative AI Services (2023)[Springer Nature, Legal and Regulatory Frameworks Governing Generative AI for Enterprises, https://link.springer.com/chapter/10.1007/978-3-032-06418-9_3, Algorithm Recommendation Management Provisions (2022)[Fei, Yang, A new regulatory framework for algorithm-powered recommendation services in China, https://www.nature.com/articles/s42256-022-00546-9], and Deep Synthesis Provisions (2023) [Library of Congress, China: Provisions on Deep Synthesis Technology Enter into Effect, https://www.loc.gov/item/global-legal-monitor/2023-04-25/china-provisions-on-deep-synthesis-technology-enter-into-effect/ accessed January 2026.

[76] Source: Author

Further, given that a JPC can transact its business beyond the schedule outlined for the parliamentary sessions, it has both the time and the ability to undertake a thorough analysis of the technical aspects of lawmaking. The closed-door and confidential nature of the JPC meetings allows room for meaningful inputs and candid discussions with experts without fear of public opinion or disclosure. A JPC also exercises broad investigative powers since it has the authority to examine witnesses under oath and compel the production of documents from government offices and private entities alike. Most notably, the JPC's recommendations, though not binding, hold high persuasive value and require the government to explain its stance on the committee's report.

The JPC, however, comes with its fair share of limitations. The timeline involved in this multiphase process must not be underestimated. The legislative journey of the DPDP Act is a prime example in this regard. The Personal Data Protection Bill, 2019 (**"PDP Bill"**), the precursor to the DPDP Act – was introduced in Parliament and referred to a JPC in December 2019[77]. The JPC submitted its report on the PDP Bill after almost two years,[78] proposing numerous amendments and recommendations. A year later, in 2022, acknowledging that the JPC's recommendations necessitated a comprehensive legal framework, the government withdrew[79] the PDP Bill and released[80] a new draft of the DPDP Bill for public consultation. The DPDP Bill received Presidential assent and finally became a law in August 2023 – after over six years since its need was first acknowledged by the Supreme Court in August 2017[81] and after almost five years since its first draft was submitted by the Srikrishna Committee in July 2018.

If needed, the AI legislation, like the DPDP Act would thereafter require drafting of Rules and a phased implementation timeline to operationalize the said AI law. We are at a juncture where we have not even contemplated the idea of setting up a JPC on AI, in which case an in-depth analysis of our present AI needs and concerns arising in the future, that culminates in a robust AI framework, seems like a distant reality.

India can benefit tremendously from the numerous benefits that a legislative instrument such as the JPC has to offer. Through its powers to investigate, review and recommend, a JPC on AI can bridge the gap between parliamentary oversight and administrative action and help determine its best approach to lawmaking on AI. India must, therefore, constitute a multipartisan JPC at the earliest to study and develop a robust regulatory regime on AI that balances innovation with regulation, and considers the competing interests of various stakeholders. This in turn shall pave the way towards effective AI governance and place India at the forefront of the AI-revolution.

[77] December 11, 2019. *See* LS, .REPORT OF THE JOINT COMMITTEE ON THE PERSONAL DATA PROTECTION BILL, 2019 https://eparlib.sansad.in/bitstream/123456789/835465/1/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf accessed Jan 2026

[78] See Economical and Political Weekly, An Assessment of the JPC Report on PDP Bill, 2019 https://www.epw.in/engage/article/assessment-jpc-report-pdp-bill-2019; SFLC, Summary of the JPC recommendations on the Personal Data Protection Bill, 2019, https://sflc.in/summary-jpc-recommendations-personal-data-protection-bill-2019/ December 16, 2021.

[79] August 3, 2022.

[80] November 18, 2022.

[81] The Supreme Court of India, in *K.S. Puttaswamy v. Union of India,* established the Right to Privacy as a fundamental right under Article 21 and called for a comprehensive data protection legislation in India.

CHAPTER 4:

National Framework for Agriculture Data Interoperability

Introduction

Employing 46.1% of the country's population and contributing around 18% to the country's GDP[82], agriculture is a focal point of the country's growth trajectory.[83] Despite the extensive scope of growth in the agriculture sector, challenges such as low productivity, fragmented landholdings, soil degradation, post-harvest losses, price volatility, and information asymmetries continue to plague the sector.

In the last decade, the agriculture sector has turned to AI technology to cultivate healthier crops, manage pests, monitor soil conditions, and analyze data for farmers. This has been accompanied by a significant growth in India's AgriTech startup ecosystem, with about 1500 startups operating across the value chain. Precision agriculture platforms such as CropIN[84] and Fasal.ai[85] provide AI-based crop monitoring, DeHaat[86] and Ninjacart[87] provide marketplace solutions connecting farmers with buyers, e-NAM platform[88] integrates agricultural markets and the Digital Agriculture Mission[89] aims to build technology driven farmer-centric ecosystem. These developments glimpse a promising future; AI driven agriculture is expected to grow at an estimated Compound Annual Growth Rate of 23% till 2028.[90]

Given the extensive operations, the sector also generates vast amounts of data. Ministries and state departments collect data on land ownership, soil health, crop patterns, irrigation, subsidies, and procurement. Similarly, private entities collect granular farm data. The data is fragmented in different formats and governed by different access rules. Such fragmented data limits the ability to generate integrated insights and be used to develop innovative AI solutions in the AgriTech sector. To resolve this bottleneck, it is imperative to build systems that enable data interoperability.

Recognizing the need for interoperability, the finance minister in the budget for FY 2026 has announced the launch of Bharat VISTAAR (Virtually Integrated System to Access Agricultural Resources) to integrate Agri Stack portals and the Indian Council for Agricultural Research package on agricultural practices with AI systems.[91] Though initiatives to build data interoperability may exist across frameworks, guidelines and initiatives, there is a need to formulate a comprehensive agricultural data interoperability framework with substantive regulatory backing. Within this context, this essay will assess the interoperability of data in existing data ecosystems and make recommendations to enable such interoperability.

Data Interoperability: Existing Data Ecosytem and Regulatory Frameworks

Agricultural Data Ecosystem

Agricultural data is collected and governed across ministries, and government departments at the Central

[82] Agriculture and Food Management, Economic Survey 2025-26, *18% contribution to GDP is attributable to Agriculture and allied services* https://www.indiabudget.gov.in/economicsurvey/doc/eschapter/echap06.pdf accessed February 2026 .

[83] PIB, *The Economic Survey 2025-26 highlights that agriculture and allied services are estimated to grow by 3.1 per cent in FY26. Ministry of Finance*, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2219912&reg=3&lang=1. accessed February 2026

[84] CropIn, https://www.cropin.com/ accessed February 2026

[85] Fasal.ai https://fasal.ai/ accessed February 2026

[86] DeHaat, https://agrevolution.in/. accessed February 2026

[87] NinjaCart, https://ninjacart.com/. accessed February 2026

[88] E-NAM, https://enam.gov.in/web/ accessed February 2026

[89] PIB ,*Digital Agriculture Mission, Tech for Transforming Farmers' Lives*, https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2051719&reg=3&lang=2 accessed February 2026 2026

[90] Down to Earth, *AI can revolutionise Indian agriculture; but it needs more investment, innovation and regulation*, https://www.downtoearth.org.in/agriculture/ai-can-revolutionise-indian-agriculture-but-it-needs-more-investment-innovation-and-regulation accessed February 2026

[91] Budget 2026-2027, *Speech of Nirmala Sitharaman, Ministry of Finance, February 1, 2026,* https://www.indiabudget.gov.in/doc/budget_speech.pdf accessed February 2026

and State level. At the Central level, the Agri Stack ('**Stack**') by the Ministry of Agriculture and Farmers Welfare under the Digital Agriculture Mission collates high quality data (functionally delegated to States) with the objective to make this data available to the stakeholders to create new services.[92] Currently, the Stack has three data blocks: a farmers' registry that captures data on farmers, crop registry hosts data on crops sown by every farmer, informed by the Digital Crop Survey, and farmland registry contains data on land held by each farmer. These categories of data repositories represents a critical interoperability layer wherein the effectiveness of repositories created hinges upon the degree to which underlying data sources adhere to consistent technical standards.

At the State level, Telangana, in August 2023, became the first State to launch an Agricultural Data Exchange **(ADeX)** in collaboration with the World Economic Forum (as a part of the AI4AI) and the Indian Institute of Science.[93] ADeX is an open-source, open-standard, and interoperable platform that facilitates secure, standards-based exchange of data between diverse data providers (government agencies, private companies,[94] NGOs, universities) and data users (AgriTech developers, startups).[95] The figure illustrates the Agricultural Data Ecosystem.

Existing Governance Measures

The agricultural data governance landscape is composed of fragmented regulatory structures, comprising both statutory law and soft instruments at the Central and State level. Illustratively, given the data collected, stored and shared, the Digital Personal Data Protection Act 2023 governs collection, storage and processing of personal data of farmers. However, it does not regulate non-personal or anonymized agricultural datasets, thereby excluding substantial categories of data that form such agricultural datasets.

Instead, agricultural data interoperability appears to be governed through soft laws such as frameworks, policies, and operational guidelines. At the national level, several policy frameworks appear to apply, however their efficacy in ensuring data interoperability warrants scrutiny. Frameworks such as the Interoperability Framework for e-Governance[96] (IFEG) set out overarching principles for building interoperability across domains.

Illustratively, the Agri Stack's repository on farmers and farmlands is governed by the Metadata and Data Standards – Demographic (**MDDS)**[97] requiring the repository to comply with technical standards enabling standardization and interoperability. While MDDS lays down the foundation for standardization, its limited applicability on demographic data leaves significant categories of agricultural information outside its ambit.

Relatedly, the implementation of Agri Stack is governed

Illustration 8: Agriculture Data Ecosystem

Agricultural Data		Agri Data Platforms/Applications		Agricultural AI Use Cases		Agricultural AI Startups	
Soil Health	Farmers' Data	Crop Registry (Digital Crop Survey)	Farmers Registry	Precision Farming	Smart Irrigation	Fasal.ai	Cropin
Landholding Data	Weather Data	Georeferenced Village Maps Registry	Krishi Decision Support System	Crop Disease Detection	Demand Forecasting	Krishi Mitra	DeHaat
Fertilisers Data	Crop Yield	Soil Health Card Portal	ADEX, Telangana	Market Price Forecasting	Predictive Analytics for Crop Yield	Nuru	EdgePlanetNet

[92] GOI, Agri Stack, https://agristack.gov.in/#/. accessed February 2026

[93] IISC, Agricultural Data Exchange (ADeX) launched in Hyderabad, Indian Institute of Science, https://iisc.ac.in/events/agricultural-data-exchange-adex-launched-in-hyderabad/February 2026

[94] Source- Authors

[95] World Economic Forum and Government of Telangana, ADex Overview, https://adex.org.in/wp-content/uploads/2023/08/ADeX-Overview.pdf February 2026

[96] Interoperability Framework for e-Governance, *Department of Electronics and Information Technology, October 2015*, https://egovstandards.gov.in/sites/default/files/2021-07/Interoperability%20Framework%20For%20e-Governance%20%28IFEG%29%20Ver1.0.pdf accessed February 2026

[97] Metadata and Data Standards – *Demographic (Person Identification and Land Region Codification), Ministry of Communication and Information Technology*, https://egovstandards.gov.in/sites/default/files/2021-07/MDDS%20Demographic%20Ver%201.1.pdf accessed February 2026

by a Memorandum of Understanding[98] between the Centre and the State government. This memorandum requires States to comply with interoperability standards set by the Centre. However, such interoperability standards were not available in the public domain, limiting researchers' ability to assess their adequacy. Other policies such as the Draft National Data Governance Framework Policy, 2022, or operational guidelines under the Digital Agriculture Mission provide policy direction, however, fail to set any technical standards for maintaining and sharing data to enable interoperability. This absence of central regulation and fragmented guidelines/standards on interoperability leads to siloed data repositories without any mandate on standards and protocols.

State-level Governance

State-led governance of agricultural data manifests through technical governance specifications, and light-touch policy frameworks. Prominently, ADeX, in Telangana, uses AgriJSON (a JavaScript-based format) for data exchange to facilitate interoperability and standardization.[99] ADeX's technical infrastructure is supported by the Agricultural Data Management Framework (ADMF)[100] which lays down the roles and responsibilities of Agricultural Information Providers (AIPs), Agricultural Information Users and Data Services Providers (DSPs). The ADMF requires AIPs and DSPs to adhere to a specified set of standards/protocols to ensure usability and interoperability.

The ADMF appears to be a siloed effort to facilitate data interoperability. While its institutional framework provides the governance scaffolding necessary for sustained interoperability, other Indian states are yet to adopt similar frameworks.

Gaps in Data Interoperability

An analysis of existing governance measures indicates that though numerous soft law instruments have been rolled out, it has not led to the formulation of a coherent interoperability regime for agricultural data in India. This has manifested gaps in India's regulatory ecosystem.

Firstly, the absence of a binding national framework leads to systemic heterogeneity in maintening agricultural data across government departments and private AgriTech companies. Currently data is collected and stored by different government departments and is subject to different technical standards, data exchange policies and access controls without an overarching mandate on interoperability. Such heterogeneity without provisions on interoperability leads to the fragmentation of data, thereby undermining the premise of data driven agricultural innovation.

Second, the mandate of existing frameworks is limited to the corresponding government registries such as AgriStack, Open Government Data Platform[101], and ADeX. Hence, private registries maintained by AgriTech entities such as AgData platform[102] are not mandated to comply with data standards leading to limited interoperability beyond themselves and government registries

Third, as agricultural data exists in multiple languages, the lack of standardization of technical terminologies may lead to semantic inconsistencies. Differences in semantics such as 'corn' and 'maize' and ontological inconsistencies such as definition of 'soil health' may make datasets non-comparable. Such incomparable datasets, when used to AI models, may lead to spurious correlations.

National Framework for Agricultural Data Interoperability

An absence of harmonized data and metadata standards may lead to diverse data schema. Therefore, there is a need for shared standards and governance to scale a unified ecosystem.[103] Fragmentation of data

[98] Digital Crop Survey, *Memorandum of Understanding between the Centre and the States*, https://agriwelfare.gov.in/sites/MinistryLettersCompendium/Digital_Crop_Survey/Implementation%20of%20DCS%20in%20all%20the%20State.pdf accessed February 2026

[99] Data to Policy Navigator, *Leveraging the power of data for agricultural resilience*, https://www.datatopolicy.org/use-cases accessed February 2026

[100] Agricultural Data Management Framework, 2023, https://adex.org.in/portfolio/agricultural-data-management-framework-admf-2023/ accessed February 2026

[101] Open Government Data Platform, https://www.data.gov.in/accessed February 2026

[102] AgData Platform, https://cropdata.in/agdata.html accessed February 2026

[103] NITI Aayog, *Reimagining Agriculture: A Roadmap for Frontier Technology Led Transformation,* November 2025, https://niti.gov.in/sites/default/

introduces significant inefficiencies such as duplication of data collection efforts, and inability to leverage cross-sectoral insights. This also leads to limiting the ability to develop AI tools that may require standardized large-scale datasets. To address the gaps in the data interoperability governance, there is a need to introduce a national framework to govern agricultural data interoperability.

Interoperability——should primarily be governed by the principles of standardization, openness (targeted at access controls), and data portability. Interoperability of data is often characterized by i) Technical Interoperability i.e., interface specifications, interconnection services, data integration services, data presentation and exchange, and secure communication protocol; ii) Semantic Interoperability relies on shared vocabulary and ontologies; iii) Organizational Interoperability requires alignment of processes; and iv) Legal Interoperability wherein legal processes do not hinder data exchange.[104] Therefore, the framework must inculcate these features.

Legal Interoperability:

The first step is to set up legal frameworks that facilitate data interoperability. Meaningful data exchange cannot be achieved without legal frameworks that authorise and enable such exchange. Therefore, to enable use of data to promote innovation in the Agri-AI ecosystem, the Ministry of Agriculture and Farmers Welfare along with the Ministry of Electronics and Information Technology should develop a National Framework for Agricultural Data Interoperability (“**Interoperability Framework**’) that will be implemented in coordination with the States.[105] Such Interoperability Framework should also lay out rights and obligations for its users. A useful precedent in this context for India is the Digital Government Law, 2021[106] in Brazil. The law, while setting an obligation on public entities to adopt open data standards, also sets out rights of citizens and public entities to access services digitally. Setting processes within the framework will enable access to such standardized data.

Technical Interoperability:

The Interoperability Framework should require adoption of open data formats such as Agri JSon, CSV, and NetCDF. Such frameworks should clearly lay out the technical standards to maintain and share data to enable interoperability. Further, all agricultural datasets should be accompanied by comprehensive metadata in alignment with the FAIR principles[107] (Findable, Accessible, Interoperable, Reusable). In the agricultural context, FAIR principles have been adopted by initiatives such as the Global Open Data for Agriculture and Nutrition (GODAN) and the CGIAR Platform for Big Data in Agriculture. This would imply developing metadata standards within the framework for agricultural data collection, and data exchange. Further, to facilitate cross-jurisdictional exchange of agricultural data, India should also align with international standards such as Agricultural Data Application Programming Toolkit (ADAPT)[108], ISO 11783[109]/ ISOXML through bidirectional conversion mechanism and India-specific extensions.

Semantic Interoperability:

Drawing from the AGROVOC,[110] India may build semantic standards wherein agricultural concepts may be mapped across languages. This assists in building an interoperable framework as agricultural datasets using different terminology could be merged for analysis by mapping their terms to the standards leading to

files/202510/Reimagining_Agriculture_Roadmap_for_Frontier_Technology_Led_Transformation.pdf.accessed February 2026

[104] European Commission, *European Interoperability Framework*, https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf accessed February 2026

[105] To build such legal systems, a law regulating data and data sharing is required, featuring the mandate on data interoperability. However, previous efforts of building central legislation/framework through the Draft Data Protection Bill 2020 and the Draft Non-Personal Data Governance Framework, 2020 were not fructified. Furthermore, given agriculture is a State subject, formulating central legislation on agricultural data may not be constitutionally prudent.

[106] Brazil, *Lei do Governo Digital, 2021,* http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14129.html. accessed February 2026

[107] Mark D. Wilkinson et al, *The FAIR Guiding Principles for scientific data management and stewardship*, https://doi.org/10.1038/sdata.2016.18. accessed February 2026

[108] ADAPT Standard, https://adaptstandard.org/docs/February 2026

[109] ISO 11783-1:2017, *Tractors and machinery for agriculture and forestry — Serial control and communications data network*, https://www.iso.org/standard/57556.html accessed February 2026

[110] AGROVOC, Food and Agriculture Organisation of the United Nations, https://www.fao.org/agrovoc/ February 2026

fragmented datasets across government departments and private entities. It also excludes datasets that are not covered within the Agri Stack mandate.

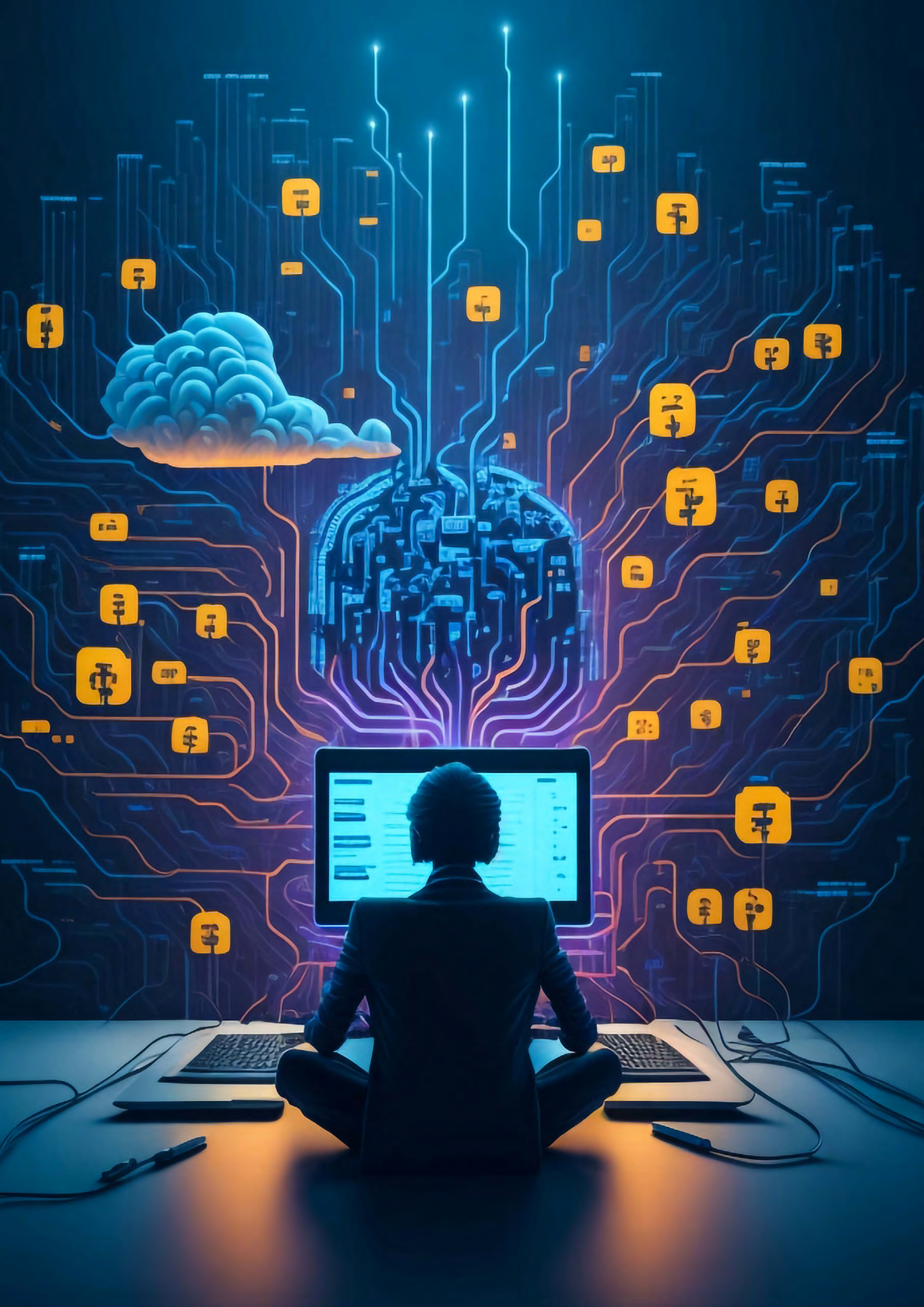
AGROVOC, Food and Agriculture Organization for the United Nations (FAO)

AGROVOC is a relevant Linked Open Data Set about agriculture to be utilized by the public. This facilitates access and visibility of data across domains and languages. One of the important aspects of AGROVOC is the structured collection of agricultural concepts, terms, definitions, and relationships that may be used to identify resources, allow standardized indexing processes, and make searches more efficient.

Organizational Interoperability

Organizational Interoperability requires alignment of processes across different departments or agencies managing agricultural data. The Interoperability Framework will standardize data processes across such departments and agencies.

Further, this framework will allow standardization in datasets created across governments and private entities and framework will pave ways to facilitate sharing and access to enable use of such standardized data repositories for developing AI models in the agricultural sector.



CHAPTER 5:

Competency Framework for Upskilling Women in the AI Ecosystem

Over the last decade, the Government of India has pursued two parallel policy tracks: gender-focused workforce initiatives and AI-focused skilling programmes. On one hand, 70 central schemes across 15 ministries and over 400 state-level schemes support female workforce participation and entrepreneurship, with gender budgets increasing by 429% from INR 0.85 lakh crore in FY 2013-14 to INR 4.49 lakh crore in FY 2025-26.[111] On the other hand, the INDIAai Mission's Future Skills Pillar aims to build AI-skilled professionals by supporting 500 PhD fellows, 5,000 postgraduates, and 8,000 undergraduates, with over 200 fellowships awarded by July 2025 across 73 institutes.[112]

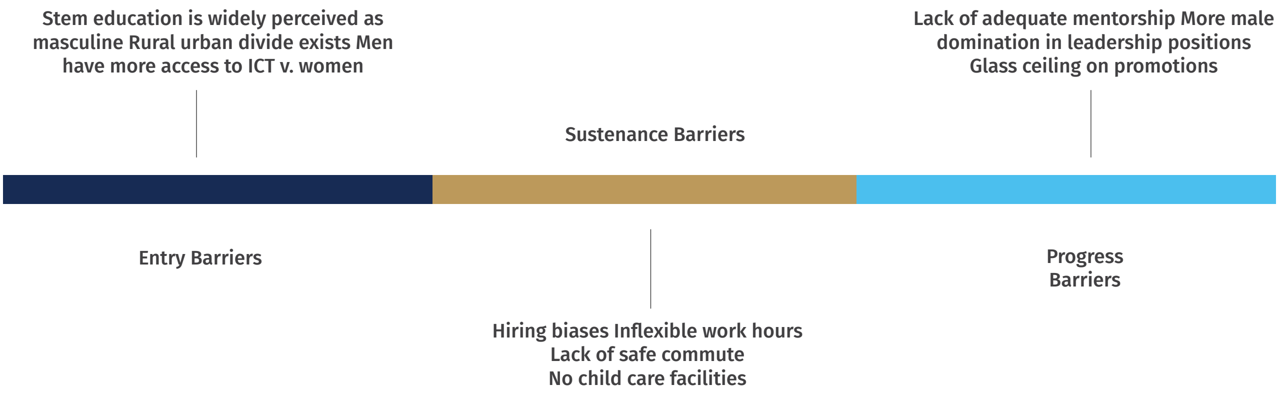
However, these initiatives have operated largely in silos. While gender-focused programmes have successfully driven a 30% increase in female self-employment, and AI skilling efforts have expanded technical capacity across the workforce, these technology-focused programmes have consistently adopted a gender-neutral approach. This is despite compelling evidence that the technology sector and AI in particular demands targeted, gender-responsive interventions.[113] Unlike other sectors where gender mainstreaming has gained traction, technology and AI skilling remains stubbornly blind to the structural barriers women face. This oversight is not incidental. Successive policy frameworks have treated digital and AI literacy as inherently accessible to all, failing to recognise that without deliberate design, such programmes will only perpetuate existing inequalities.

Structural Barriers for Women in Tech

Women in India's technology sector face systemic and lifecycle barriers in tech. These barriers maybe presented as three key themes: entry barriers, sustenance barriers and progress barriers.

First, entry barriers start with STEM education being widely perceived as masculine, with dominant narratives about femininity discouraging women from pursuing science and mathematics.[114] Further, due to the rural-urban divide, women in rural areas, are 31% less likely than men to use mobile internet, to even access technology in the first place. Cultural norms, cost, and safety concerns further restrict access, contributing to women representing only 25% of STEM college students.[115] Further, women from marginalized regions, castes, or linguistic backgrounds

Illustration 9: Structural Barriers for Women in Tech


Stem education is widely perceived as masculine Rural urban divide exists Men have more access to ICT v. women
Lack of adequate mentorship More male domination in leadership positions Glass ceiling on promotions
Sustenance Barriers
Entry Barriers
Progress Barriers
Hiring biases Inflexible work hours
Lack of safe commute
No child care facilities

[111] PIB, *Nari Shakti se Viksit Bharat: Women Leading India's Economic Transformation Story*,https://www.pib.gov.in/PressReleasePage.aspx?PRID=2160547®=3&lang=2 accessed February 2026

[112] *Ibid.*

[113] United Nations Industrial Development Organisation,, *Gender Digital Transformation and Artificial Intelligence*,https://hub.unido.org/sites/default/files/publications/GENDER%2C%20DIGITAL%20TRANSFORMATION%20AND%20AI%20REPORT.pdf accessed February 2026

[114] The Quantum Hub, *Women in Stem Challenges and Opportunities in India*, https://thequantumhub.com/women-in-stem-challenges-and-opportunities-in-india/# accessed February 2026

[115] Frontiers In, *The Gender Gap in STEM Fields:The Impact of the Gender Stereotype of Math and Science on Secondary Students' Career Aspirations*, https://www.frontiersin.org/journals/education/articles/10.3389/feduc.2019.00060/full. accessed February 2026

face compounding obstacles, as most skilling initiatives are urban-focused, with instructions being carried out in English.[116] Women from scheduled caste/scheduled tribe communities, moreover, have lower ICT access, placing them at an immediate disadvantage.[117]

Second, there are certain sustenance barriers. These include hiring biases that unfairly disadvantage women with certain ailments. For instance, 36.5% of women aged 25 - 40 suffer from anaemia, impairing cognitive function and fuelling discriminatory hiring.[118] Age-restricted grants disadvantage women with care responsibilities, while credential-focused hiring favor elite institutes where women are underrepresented (only about 15-18% at IITs[119]).

Soft skill initiatives do not account for the fact that men are able to dedicate significantly more time (19.9%) to employment-related activities than women (4.9%).[120] Skilling programmes lack childcare accommodation, modules on soft skills and workplace culture, and solutions for mobility challenges. Distressingly, 15.5% women drop job/skilling opportunities due to commuting difficulties. Further, women in technology face every day biases including trivialization of their work, assignment of menial tasks, and exclusionary policies such as escort rules. A survey by FlexJobs in 2022 revealed that 56% of women cited lack of flexibility as the primary reason for not returning to the workforce after a career break.[121] Despite robust work-from-home arrangements, flexible working policies often exaggerate unpaid care burdens, reduce visibility for promotions (94% of remote workers fear that they are less likely to be promoted), and increase isolation and burnout.[122] Rapid technological change, workplace rigidity, and scarce returnship programmes (only 35% companies offer them) hinder women's re-entry.[123]

Third, there are barriers to progress. Studies show that formal mentorship for women is rare; and informal networks are male dominated. While 75% of senior women credit mentorship for their success, only 37% have access to structured mentoring.[124] Women also face a glass ceiling with their promotions. For instance, women constitute 51% of entry-level IT recruits but only 25% of managers and less than 1% of top leadership. Only 7% of Indian tech executives are women, despite comprising 36% of employees - reflecting cultural biases that perceive women as less committed, particularly after marriage and motherhood.[125] Specifically, it has been documented that the tech industry suffers from a lack of visible female role models and mentors. Without women in higher positions to inspire, guide, and advocate for them - aspiring female technologists feel isolated and less inclined to persevere in the face of challenges, exacerbating the skills gap.[126]

Addressing these systemic barriers - entry barriers, sustenance barriers, and progress barriers, in the context of AI, is not merely important but urgent, and this urgency is driven by twin objectives. AI represents the next great technological revolution, and history has shown that revolutions of this kind do not disrupt existing biases; they deepen them. If left unaddressed, entry barriers risk shutting women out of the AI race entirely, while sustenance and progress barriers ensure that those few who do gain a foothold are unable to remain or advance. The same patterns of exclusion that have characterised previous technological shifts will be replicated and amplified at unprecedented scale.[127]

[116] UNICEF, *Digital Equality for Girls, South Asian Imperative,* https://www.unicef.org/rosa/stories/digital-equality-girls-south-asian-imperative accessed February 2026

[117] Adhyaan Foundation, *Caste-based Inequities in Digital Access,* https://afpr.in/caste-based-inequities-in-digital-access/ accessed February 2026

[118] Loop Health, *India Workforce Health Ind*: https://whi.loophealth.com/ accessed February 2026

[119] Ideas for India, *Girls in Tech: Evaluating IITs Supernumerary Seats,* https://www.ideasforindia.in/topics/social-identity/girls-in-tech-evaluating-iit-s-supernumerary-seats-scheme accessed February 2026

[120] Shilpi Verma,In 2019, women in India spent an average of 299 minutes each day on unpaid domestic services. This was thrice the time spent by men on similar services. Our vision is to take India forward one Kraft at a time. An aware India knows that transformation of governance cannot happen without the transformation of mindset, available at: https://www.bluekraft.in/wp-content/uploads/2025/06/Shilpi-Verma-2.pdf accessed February 2026

[121] IJCRT, *Challenges Faced by Women in the IT Sector After a Career Break, in the Context to Coimbatore City*,: https://ijcrt.org/papers/IJCRT2507367.pdf accessed February 2026

[122] Deloitte, *Working women face alarmingly high levels of burnout despite shifting work arrangements, rise in hybrid working*,: https://www.deloitte.com/in/en/about/press-room/men-face-alarmingly-high-levels-of-burnout-despite-shifting-work-arrangements-rise-in-hybrid-working.html accessed February 2026

[123] Centre For Economic Data and Analysis, *Return to Work*, https://backend.udaiti.org/wp-content/uploads/2025/02/Return-to-Work.pdf accessed February 2026

[124] Economic Times, *Closing the leadership gap: Why skilling women for the future is a business imperative*, https://etedge-insights.com/c-suite-corner/leadership/closing-the-leadership-gap-why-skilling-women-for-the-future-is-a-business-imperative/ accessed February 2026

[125] McKinsey & Company, *Women in Workplace, McKinsey*,: https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/women-in-the-workplace accessed February 2026

[126] Womentech Network, *Why Aren't There More Women in Tech Exploring Skills Gap*,: https://www.womentech.net/how-to/why-arent-there-more-women-in-tech-exploring-skills-gap accessed February 2026

[127] UNESCO, Challenging systematic prejudices: an investigation into bias against women and girls in large language models, available at: https://unesdoc.unesco.org/ark:/48223/pf0000388971 accessed February 2026

However, AI also presents a profound opportunity: if developed responsibly, by diverse teams committed to positive societal impact, and if harnessed ethically and inclusively, it has the potential to actively advance the aims of gender equality and equity worldwide.[128] AI systems designed to mitigate rather than perpetuate inequality and gender disparity in their interactions with society could become powerful instruments of change.

Drawbacks of the Current Approach to Upskilling

Observably, women face structural barriers that gender neutral approaches to skilling have had difficulties in resolving. These bottle-necks are also interwoven in other social issues like caste, language, religion and socio-economic status, amongst others – exacerbating women's challenges to access training and skilling. While traditional approaches to skilling have managed to increase participation in STEM and AI training, conversion into sustained employment, seniority, and leadership remain disproportionately low.

Gender Neutral Design

The GoI's FutureSkills Program espouses the vision of *"AI for All"* and has made strides in expanding access - with 27 AI labs planned across smaller cities and fellowships awarded to undergraduate and postgraduate student. However, their approach to upskilling women in smaller cities remain largely gender-neutral in design and do not adequately address the structural bottlenecks that demerit women. These could include – commuting problems, child-care concerns, lack of mentorship and others. Something as forward looking as National Apprenticeship Training Scheme[129], a scheme that intends to empower the youth through training, does not include gender-based considerations in their training modules. It leaves out important soft skills for women like workplace boundaries, confidence in male-dominated environment, strategic networking and ally building.

Lack of Coherent Regulatory Intent

Beyond programme design, India's AI and technology skilling ecosystem also suffers from a lack of coherent regulatory intent and coordination. Skilling initiatives are fragmented across central ministries, state governments, and sectoral bodies, with limited harmonisation of objectives, standards, or outcomes. For example, while MeitY's FutureSkills PRIME programme[130] focuses on advanced AI, cloud, and emerging technology roles, with nationally standardised certifications delivered through select industry partners; states such as Karnataka simultaneously run independent digital and technology skilling programmes through bodies like the Karnataka Skill Development Corporation[131] (KSDC) and Karnataka Digital Economy Mission (KDEM).

While central schemes articulate broad national visions, states independently design and implement training programmes based on local priorities and capacities, resulting in uneven quality and duplication of efforts. In the absence of a unifying framework or vision statement backed by regulatory guidance, gender-responsive objectives remain discretionary rather than mandatory. As a result, initiatives that meaningfully address women's specific barriers tend to emerge as isolated, pilot-driven interventions rather than system-wide design features.

The Need for a Gender-Responsive AI Competency Framework

The evidence above demonstrates that the shortcomings of India's AI and technology skilling ecosystem stem not from a lack of programmes or investment, but from the absence of a structuring mechanism that aligns skilling with lived realities, labour market outcomes, and equity objectives. For structured alignments, jurisdictions across the world are exploring competency frameworks for different domains.

A **competency framework** is a structured model that defines the *knowledge, skills, attitudes, and behaviours* needed to perform effectively in each domain, often mapped across progressive levels of proficiency. It provides a common language for policymakers, educators, employers, and learners to align training, assessment, and market expectations. For example, the European Union's Digital Competence Framework[132] (DigComp) provides a common reference for digital skilling across member states by defining core digital competencies and progressive proficiency levels.

The GSMA Gender Transformative Digital Skills

[128] *Ibid.*

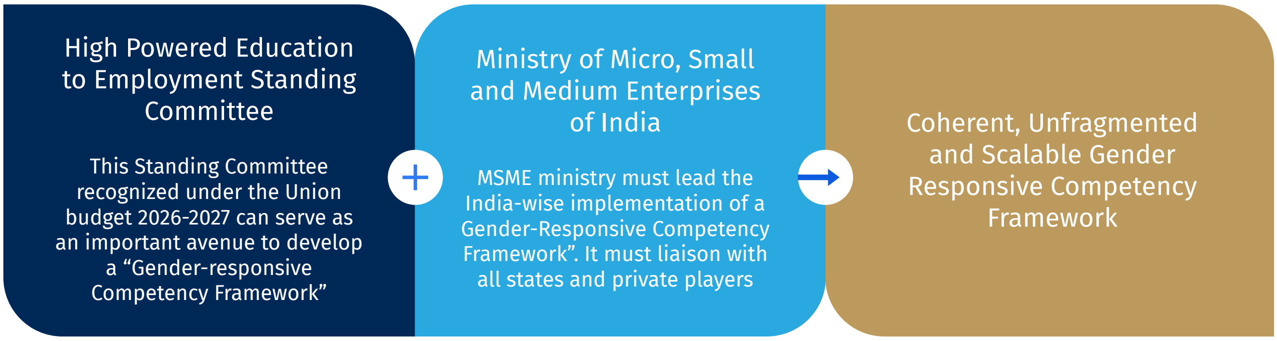
[129] National Training Apprenticeship Scheme, https://nats.education.gov.in/about-us.php accessed February 2026.

[130] Future Skills Prime, https://www.futureskillsprime.in/ accessed February 2026

[131] Karnataka Skill Development Corporation, https://kaushalkar.karnataka.gov.in/en accessed February 2026

[132] Digital Transformation in Education, Digi Comp Framework, a https://joint-research-centre.ec.europa.eu/projects-and-activities/education-and-training/digital-transformation-education/digital-competence-framework-digcomp/digcomp-30_en accessed February 2026

Illustration 10: Suggested Implementation Plan for a Gender-Responsive Competency Framework



High Powered Education to Employment Standing Committee

This Standing Committee recognized under the Union budget 2026-2027 can serve as an important avenue to develop a "Gender-responsive Competency Framework"

Ministry of Micro, Small and Medium Enterprises of India

MSME ministry must lead the India-wise implementation of a Gender-Responsive Competency Framework". It must liaison with all states and private players

Coherent, Unfragmented and Scalable Gender Responsive Competency Framework

Framework[133], for instance, explicitly addresses social norms, structural barriers, and lifecycle constraints that shape women's participation in digital economies, shifting focus from access alone to sustained economic outcomes. While not AI-specific, it demonstrates how competency frameworks can be intentionally designed to reduce gender disparities rather than remain neutral to them. Similarly, by developing a central "*Gender-responsive AI competency Framework*", India has the opportunity not only to address its domestic skilling gaps but to set a replicable model for the Global South where similar demographic, social, and labour market constraints shape women's participation in emerging technology.

The Indian Union Budget 2026-27 presents an important avenue. The proposal to establish a "High-Powered Education to Employment and Enterprise Standing Committee"[134] (**Standing Committee**) tasked with recommending measures to assess the impact of AI on jobs and skill requirements, provides an institutional mechanism through which these concerns can be operationalised. In discharging its mandate, the Standing Committee should recommend a "*Gender-Responsive Competency Framework*". Once recommended, the Ministry of Micro, Small and Medium Enterprises must take forward this gender-responsive competency framework as a national baseline framework for AI upskilling in India. Given the Ministry's deep reach into the economic fabric of the country and its direct engagement with other states, entrepreneurs, small businesses, it is uniquely positioned to ensure adoption of the framework across states and to drive its integration within the private sector. This would embed gender-responsive AI upskilling not only within government programmes but also within the practices of enterprises and industries nationwide, creating a coherent, unfragmented and scalable pathway from policy recommendation to ground-level impact.

Below we outline a suggested framework for the Standing Committee's consideration - to showcase India's Competency Model, given its unique realities.

[133] UNICEF, Towards a Gender Transformative Approach, https://www.equalsintech.org/_files/ugd/04bfff_e5af5fd767394022be9065767b7028d6.pdf accessed February 2026

[134] Union Budget 2026-27 , Proposes High-Powered *'Education To Employment And Enterprise'* Standing Committee to Recommend Measures on the Services Sector, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2221405&reg=3&lang=2. accessed February 2026

ANNEXURE – CHAPTER 5

Suggested Gender Responsive AI Competency Framework for Women[138]

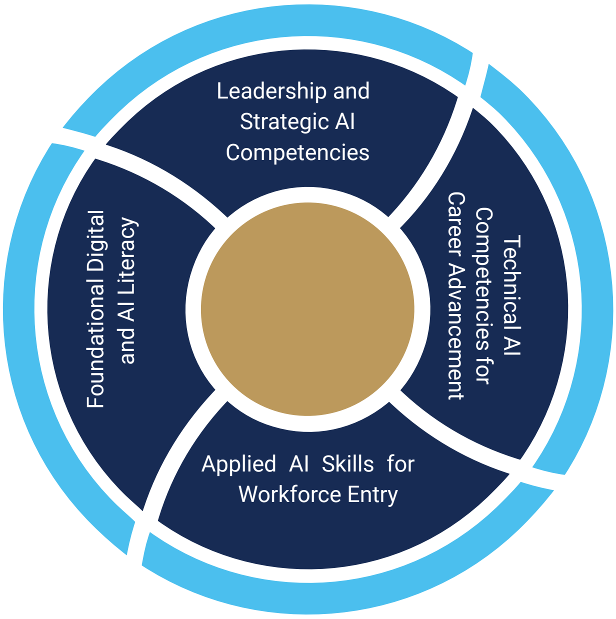
Preamble: The following framework intends to offer a starting point for designing any skilling-based initiative for women. The framework is organized across four dimensions, with specific evaluation metrics mapped across three proficiency levels (basic, intermediate and advanced).

Methodology: The competency framework is derived directly from the barriers identified in the preceding sections, ensuring that the framework responds to real and observed constraints rather than abstract skill gaps. These barriers are clustered into four key dimensions of competency. Each dimension captures a distinct capability required for meaningful participation and sustained engagement of in the skilling ecosystem.

For each dimension, we define inclusion evaluation metrics with use cases. Rather than relying solely on input-based indicators (such as hours of training or content coverage), the framework emphasises outcome-based assessment. These outcomes are framed as observable behaviours or task completions that can be consistently evaluated across cohorts. To operationalise evaluation, we pair each evaluation metric with context-specific use cases. These use cases translate abstract competencies into real-world scenarios in which learners must demonstrate comprehension, decision-making, or task completion under typical programme conditions.

Overview of the Dimensions

Illustration 11: Overview of the Dimensions


Leadership and Strategic AI Competencies
Technical AI Competencies for Career Advancement
Applied AI Skills for Workforce Entry
Foundational Digital and AI Literacy

Dimension 1: Foundational Digital and AI Literacy for Women [as this is a suggested framework. We Map Out Only One Dimension]

Levels	Inclusion Evaluation Metrics	Use Cases
Basic	**Evaluation Metric 1:** Vernacular Accessibility and Linguistic Inclusion **Measurement Criteria:** At least **80 - 100% of core instructional content** (videos, readings, assessments) is available in **one or more local languages** relevant to the target region. Use of **voice-based or speech-enabled interfaces** for low-literacy participants. Presence of **locally trained facilitators** capable of delivering instruction in regional dialects.	**Use Case:** A state government partners with local self-help groups to deliver an AI literacy programme for rural women entrepreneurs in the handicrafts sector. The programme provides all instructional content - including video tutorials on using AI tools for inventory management, pricing, and market analysis in regional languages such as Odia, Assamese, and Marathi. For participants with limited literacy, the platform incorporates voice-based navigation and audio explanations, enabling them to interact with learning materials through simple spoken commands.

[135] This framework has been developed after a literature review of global competency frameworks in EU and others.

Levels	Inclusion Evaluation Metrics	Use Cases
	Evaluation Metric 2: Care-Aware and Hyperlocal Delivery Design **Measurement Criteria:** • Proportion of learning hours that can be completed **asynchronously or remotely** (minimum threshold - 50%). • Availability of **on-site or subsidised childcare** for all in-person sessions, or formal partnerships with local childcare providers. • Average distance of physical training centres from participants' residences (like within walking distance or short public transport commute).	Locally recruited facilitators, drawn from the same communities, conduct weekly in-person sessions at village community centres, offering guidance in regional dialects and contextualising AI applications to local business practices such as seasonal demand forecasting for traditional textiles. **Use Case:** A publicly funded AI skilling programme designed for women caregivers offers modular coursework, flexible deadlines, and mobile-first access. Participants many of whom balance paid work and unpaid caregiving are able to pause and resume lessons without penalty, attend short live sessions scheduled outside peak caregiving hours, and access recorded content in local languages.
Intermediate	**Evaluation Metric:** Demonstrate Functional Understanding of Basic AI Concepts **Measurement Criteria:** • Proportion of women learners demonstrating functional understanding of basic AI concepts. • Proportion of women learners correctly identifying AI-enabled tools in their daily lives and work contexts, explaining their purpose in simple terms, and making informed choices about their use without reliance on technical jargon or English-language explanations.	**Use Case:** In a foundational AI literacy programme for women re-entering the workforce, participants are able to accurately distinguish AI-driven applications from non-AI tools, articulate their function in their preferred language, and apply this understanding to a practical choice (like adjusting app settings or deciding whether to rely on an automated recommendation).
Advanced	**Evaluation Metric:** Demonstrate data awareness and Critical Digital Judgment **Measurement Criteria:** Proportion of women learners demonstrating data awareness and critical digital judgment by accurately identifying personal data, recognising privacy risks, and assessing AI-generated content for reliability and potential bias Number for women taking at least one informed action to protect their data or challenge an automated output.	**Use case**: In a community-based digital skilling programme, participants are given common digital tasks, such as installing a mobile app or reviewing an AI-generated message. They correctly point out which information requested is personal, briefly explain one reason why sharing it may be risky, and choose an appropriate action such as allowing only essential permissions, changing a privacy setting, or checking the information with another source before acting on it. Participants complete these steps using their preferred language and without facilitator assistance, demonstrating every day, usable judgment in interacting with AI-enabled tools.

Notes

Notes

Authors

This publication has been authored by the following members from Shardul Amarchand Mangaldas & Co.

Dr. Shardul S. Shroff
Executive Chairman

KS Roshan Menon
Principal Associate

Lakshita Bhargava
Associate

Shruthi Nair
Associate

Ridhima Saxena
Associate

Geetanjali Bisht
Associate

Himali Sylvester
Associate

Acknowledgements

This publication was prepared under the aegis of Shardul Amarchand Mangaldas & Co (SAMCo). We thank ***Dr. Shardul S. Shroff****, Executive Chairman at Shardul Amarchand Mangaldas & Co, for his support and invaluable guidance throughout the development of this volume. We are also grateful for the valuable contributions of the SAM In-house Design Team, including* ***Chitersen Shisodia****, Associate Director – Creatives, and* ***Cruz Sahaya****, Assistant Manager – Graphic Designer.*

In addition to the authors listed above, we wish to acknowledge the diligent contributions of ***Aryan R. Nair****,* ***Siddharth Malik****, and* ***Vaishnavi Singh****, who provided invaluable research and editorial assistance.*

Disclaimer

This publication has been prepared by Shardul Amarchand Mangaldas & Co. ("SAM") for general informational purposes only and does not constitute legal, tax, financial or any other professional advice. The information has been compiled from sources believed to be credible; however, it is provided on an "as is" basis without any representation or warranty, express or implied, as to its accuracy or completeness, and SAM shall not be liable for any loss arising from reliance on this publication. Readers are advised to seek appropriate professional advice before taking any action.

All images used in this publication have been sourced from www.freepik.com and are used for illustrative purposes only.