INTOSAI

SUPREME AUDIT INSTITUTION OF INDIA
लोकहितार्थ सत्यनिष्ठा
Dedicated to Truth in Public Interest

# PursuIT

an **INTOSAI WGITA** e-Journal

# DIGITAL PUBLIC INFRASTRUCTURE

## An Enabler for Inclusive Governance




iCISA
INTERNATIONAL CENTRE FOR INFORMATION SYSTEMS & AUDIT
A Global Capacity-Building Centre of C&AG of India

11th Edition
(September 2026)




# INTERNATIONAL CENTRE FOR INFORMATION SYSTEMS & AUDIT

A Global Capacity-Building Centre of C&AG of India

# TABLE OF CONTENTS


| | | |
|---|---|---|
| 1 | **Message from the Comptroller and Auditor General of India** | 7 |
| 2 | **Message from the Director General, iCISA** | 9 |
| 3 | **Section I — Foundations: DPI as a Governance Construct** | 11 |
| I | From Identity to Inclusion: How India Built Digital Public Infrastructure as an Enabler of Inclusive Governance - *Aashita Dagar, India* | 12 |
| II | How Digital Systems Become Public Infrastructure: DPI Transformability and the Institutional Conversion of Digital Public Infrastructure - *Kentaro Saito, Japan* | 23 |
| III | Digital Public Infrastructure as an Enabler of Inclusive Governance: Mechanisms, Evidence, and the Audit Imperative - *Harsha Bhowmick & Abhishek Singh, India* | 39 |
| IV | From India Stack to Citizen Stack: India's DPI Journey and a Blueprint for the World - *Karan Vohra & Keshav Bhardwaj, India* | 51 |
| 4 | **Section II — The Layers Beneath: Connectivity, Cloud and Location** | 60 |
| I | Mapping Municipal Equity: Leveraging Spatial DPI for Inclusive Solid Waste and Utility Management in Smart Cities - *Dr. Nanda Dulal Das, India* | 61 |
| II | Auditing the Connectivity Layer of Digital Public Infrastructure: Lessons from BPK's Performance Audit of the Indonesian Telecommunications Infrastructure Regulatory Agency - *Benidiktus Bambang Triasmoro, Dwi Jatmika Bima Mahatmantara, Arief Ridhatama, Achmad Faishal & Amri Lewa, Indonesia* | 71 |
| III | Digital Public Infrastructure and Cloud Computing: GAO Identified Challenges - *Jonnie Genova & Jess Lionne, United States of America* | 82 |
| 5 | **Section III — DPI in the Sectors: Service Delivery on the Ground** | 87 |
| I | AgniDrishti: An AI-Enabled Fire Risk Intelligence System as Digital Public Infrastructure for India's Fire and Emergency Services - *Tania Mishra, India* | 88 |
| II | Digital Public Infrastructure for Inclusive Governance: The EASE Platform for Citizen-Centric Entitlement Services in Jharkhand, India - *Bhargav Ram Khyathi, India* | 101 |
| III | Who Benefits from Digital Public Infrastructure? Auditing Inclusion, Accountability, and Service Delivery Outcomes - *Maha Fathy Ibrahim Morsy, Egypt* | 112 |
| IV | From AI Access to Ethical Readiness: Auditing AI-Enabled Education DPI for Inclusive Governance: Reflections from India Stack and Uzbekistan's Emerging Experience - *Rustamkhuja Ishanov, Uzbekistan* | 118 |

**6 Section IV — The Inclusion Test: Making Exclusion Visible and Verifiable** 125

I Diagnosing and opening the black-box of Digital Public Infrastructure: A Process-Audit Approach to Inclusive Governance — *- Chakradhar Buddha & Dr. Rajendran Narayanan, India* 126

II Inclusion by Verification: Why Digital Public Infrastructure's Promise of Inclusive Governance Depends on a Dedicated Data-Reliability Audit Approach — *- Jishnu J Raju, India* 137

III Extending the Use of Audit Data Can Help Strengthen Inclusivity — *- Sandeep Radhakrishnan, India* 149

IV Auditing Digital Public Infrastructure for Inclusive Governance: Insights from India's Direct Benefit Transfer Experience — *- Sameer Asif, India* 156

**7 Section V — The Audit Response: Frameworks, Guidelines and Field Experience** 168

**V-A Frameworks and Guidelines** 169

I Auditing Decision Accountability in AI-Enabled DPI: Lessons from a Social Impact Study of Welfare Schemes in India — *- BK Mohanty, Krishnan Narayanan & VR Muraleedharan, India* 170

II Auditing Digital Public Infrastructure: Strengthening Inclusive Governance through Supreme Audit Institutions — *- Serah Kituu, Kenya* 182

III Beyond IS Audit: Auditing the Invisible Architecture of Digital Public Infrastructure — *- Ajay Yeshwanth, India* 193

IV Digital Public Infrastructure as an Enabler of Inclusive Governance: Opportunities, Risks, and the Role of Audit — *- Pranay Chauhan, India* 200

**V-B Field Experience** 207

I Auditing Digital Public Infrastructure: Lessons from TCU (SAI Brazil) on Quality Assessment of Selected Federal Digital Services — *- André Luiz de Albuquerque Farias, Brazil* 208

II Digital Public Infrastructure as an Enabler for Inclusive Governance — *- Malik Sulaiman Hamood Al Ghawi, Oman* 219

III Auditing Digital Public Infrastructure During Implementation: Lessons from Brazil's Gestão Presente System (SGP) — *- Klauss Nogueira, Fernando Faria, Harley Ferreira & Rafael Albuquerque, Brazil* 226

**8 Section VI — Country Journeys: Building DPI in Emerging Environments** 236

I Digital Public Infrastructure as an Enabler of Inclusive Governance: An Audit Perspective from Sierra Leone — *- Abu Allicious Gogra-Hilton, Sierra Leone* 237

II The Technological Crossroads: Challenges and opportunities of Digital Public Infrastructure in Cuba — *- Makisleidis Esponda Bravo, Cuba* 247

| | | |
|---|---|---|
| 9 | **Section VII — The Next Horizon: AI, Digital Twins and Anticipatory Assurance** | 254 |
| I | Auditing Digital Public Infrastructure in the Age of Artificial Intelligence: A Vietnamese Perspective on Moving toward Proactive Public Audit<br>*- Tran Thi My Giang, Vietnam* | 255 |
| II | Building Tomorrow, Today: How Digital Twins are reshaping India's Infrastructure journey to 2047<br>*- Piyush Tiwari, India* | 264 |
| 10 | **Our Contributors** | 279 |
| 11 | **Global Capacity Building Initiatives of SAI India** | 299 |

# MESSAGE FROM THE COMPTROLLER AND AUDITOR GENERAL OF INDIA



It gives me immense pleasure to present the inaugural edition of the *INTOSAI Working Group on IT Audit (WGITA) e-Journal*, on the theme ***"Digital Public Infrastructure (DPI): An Enabler for Inclusive Governance."***

The launch of this e-Journal is an important step in WGITA's endeavour to foster knowledge sharing, professional cooperation and exchange of experiences among Supreme Audit Institutions (SAIs) in the rapidly evolving digital landscape. As digital technologies increasingly shape public administration, the role of SAIs in providing independent assurance on the governance of digital systems has assumed greater significance.

Digital Public Infrastructure has emerged as a powerful enabler of inclusive, efficient and citizen-centric governance. India's experience demonstrates the transformative potential of DPI when developed as an interoperable and scalable public digital good. Platforms such as **Aadhaar, UPI, Jan Dhan, Direct Benefit Transfer, PFMS, DigiLocker and GeM** have enabled digital identity, financial inclusion, payments, public financial management and delivery of public services at unprecedented scale. In January 2026 alone, UPI recorded 21.70 billion transactions, while the cumulative value of Direct Benefit Transfers has crossed ₹49 lakh crore (514.5 billion USD). Such scale illustrates the potential of digital infrastructure to improve access, efficiency and transparency in governance.

However, the success of DPI cannot be measured by scale and transaction volumes alone. Its true value lies in its ability to leave no one behind, improve outcomes, protect citizens' interests and strengthen trust in public institutions.

For SAIs, this transformation brings both opportunities and new responsibilities. Audit approaches must evolve to examine not only financial transactions and outcomes, but also the data, systems, controls, interoperability, cybersecurity, privacy, resilience and accountability that underpin digital governance. Technology-enabled audit and data analytics can provide new avenues for strengthening public accountability while complementing the fundamental principles of public-sector auditing.

I am pleased to note that the Editorial Team of the Journal comprises representatives from India, the Republic of Korea and South Africa, reflecting the spirit of INTOSAI and the value of sharing diverse experiences and perspectives. My appreciation goes to all the authors and members of the Editorial Team whose contributions have enriched this inaugural edition.

I hope this e-Journal will serve as a meaningful platform for professional dialogue, exchange of experiences and dissemination of good practices, and stimulate further collaboration among SAIs.



**K. Sanjay Murthy**
**Comptroller & Auditor General of India**

# MESSAGE FROM THE DIRECTOR GENERAL, iCISA



Digital transformation is fundamentally changing the way public institutions function and citizens access government services. At the centre of this transformation is Digital Public Infrastructure (DPI), which is increasingly emerging as a critical foundation for efficient, accessible and inclusive governance. It is in this context that the 11th edition of *PursuIT* focuses on the theme ***"Digital Public Infrastructure: An Enabler for Inclusive Governance."***

This edition marks an important step in the journey of *PursuIT*. Building upon the previous edition, which featured contributions from eight Supreme Audit Institutions (SAIs), the present edition brings together 12 international contributions. From this edition onwards, the journal is being published as the official INTOSAI WGITA e-Journal, further strengthening its international recognition. The Editorial Board has also been expanded to include members of the international auditing fraternity, with representation from the Republic of Korea and South Africa, reinforcing the journal's role as a platform for cross-border professional exchange.

The growing importance of DPI has also been reflected in the initiatives undertaken by iCISA, the international training institute of SAI India and also the Global Training Facility of WGITA to facilitate capacity building and knowledge-sharing in this emerging area. The 166th International Training Programme on **"Audit of Digital Public Infrastructure"**, conducted in November 2025, brought together participants from 26 countries, providing a forum for sharing experiences and examining the evolving approaches to auditing DPI. iCISA has further encouraged professional dialogue through initiatives such as panel discussion on DPI, enabling practitioners to engage with the opportunities, risks and emerging audit considerations associated with digital public systems.

As DPI continues to shape the delivery of public services, auditors must develop the ability to assess not only the technological foundations of these systems, but also their inclusiveness, effectiveness, security, accountability and impact on citizens. I hope that the articles in this edition will enrich this discourse and provide useful insights to the SAI community.

I extend my appreciation to all the contributors, authors, reviewers and Editorial Board members whose efforts have made this edition possible, and look forward to *PursuIT* continuing its journey as a forum for professional learning and collaboration.



**Bijay Kumar Mohanty,**
**Director General, iCISA**
**CTO, O/o the CAG of India**



Section I

# FOUNDATIONS: DPI AS A GOVERNANCE CONSTRUCT

# From Identity to Inclusion: How India Built Digital Public Infrastructure as an Enabler of Inclusive Governance

*A Practitioner-Informed Case Study of Aadhaar, Payments, Finance and Public Service Platforms*

**Aashita Dagar**
Principal Consultant,
National e-Governance Division, DIC, MeitY,
Government of India



## Abstract

Over less than two decades, India has assembled one of the world's most important portfolios of Digital Public Infrastructure, a layered set of foundational platforms that now mediates identity, payments, public finance and welfare delivery for more than a billion people. This article traces that journey across the platforms that make up the stack: Aadhaar, the Unified Payments Interface (UPI) and the National Payments Corporation of India (NPCI), the Public Financial Management System (PFMS), the Pradhan Mantri Jan-Dhan Yojana (PMJDY), the Government e-Marketplace (GeM), the Goods and Services Tax Network (GSTN), the Ayushman Bharat Digital Mission (ABDM) and the eSanjeevani telemedicine platform. It traces the context that made reform necessary. fragmented identity, low banking penetration, leakage-prone welfare and opaque, paper-based administration, and shows how a deliberate "think platforms, not projects" philosophy produced reusable, interoperable rails. India's DPI succeeded through several reinforcing choices: building foundational layers others could build upon; using existing institutional and financial mechanisms to move quickly; retaining public control of mission-critical functions while outsourcing the rest under enforceable contracts; and embedding equity, openness and accountability from the outset. For Supreme Audit Institutions, this reframes the audit question from whether a single system works to whether a shared public platform is governed by a clear legal mandate, secure, resilient and inclusive by design. The Indian experience offers a transferable template for inclusive governance, while raising new questions about data protection, algorithmic and biometric auditability, vendor concentration and institutional durability.

## Keywords

Digital Public Infrastructure; Inclusive Governance; Aadhaar; Unified Payments Interface (UPI); Direct Benefit Transfer (DBT); Public Sector Audit

## 1. Introduction

Inclusive governance depends on a deceptively simple capability: the state's ability to recognise a citizen, transfer a benefit, collect a tax or deliver a service reliably and at scale. For much of India's post-independence history, this capability was constrained by structural gaps. Large segments of the population lacked reliable proof of identity; only about a third of adults held a bank account; welfare reached beneficiaries through long, leaky chains; and procurement and tax administration were fragmented across paper-based, locally administered systems. The cumulative cost was measured not only in money but in exclusion of the rural poor, migrants, women and those at the bottom of the economic pyramid.

The response that emerged from the late 2000s onward was not a single program but an architecture. India chose to build Digital Public Infrastructure (DPI): shared, foundational digital systems for identity, payments and data exchange, that public and private actors could build upon, much as roads or electricity grids enable a wide range of downstream activity. Unlike a conventional e-governance project, which digitises one department's process, DPI is a horizontal, reusable layer exposing open standards and interfaces, interoperable across institutions and designed to be built upon by parties the original designers never anticipated. The Indian formulation organises these as a presence-less identity layer, a paperless documents layer, a cashless payments layer and a consent-based data layer, popularly known as the India Stack. This article examines that architecture through the design and implementation history of its components, as documented in the Digital Transformation (DPI) Podcast series produced by the National e-Governance Division (NeGD), setting out the need and design logic behind each platform and drawing out the implications for the international community of Supreme Audit Institutions (SAIs).




**Figure 1.** *The India Stack, the layered architecture of India's Digital Public Infrastructure, comprising presence-less (identity), paperless (documents), cashless (payments) and consent (data) layers.*
*Source: based on the UPI / NPCI podcast deck, NeGD Digital Transformation (DPI) series.*

## 2. The Foundational Layer: Aadhaar and Digital Identity

The cornerstone of India's DPI is Aadhaar, the unique biometric identity issued by the Unique Identification Authority of India (UIDAI). Before Aadhaar, identity in India was a patchwork: agencies issued their own identifiers with no standardisation and no safeguards against duplication, and there was no way to verify authenticity online in real time. The result was exclusion for those who could not prove who they were, fraud where a single person could claim multiple benefits, and enormous administrative cost in repeatedly re-establishing identity.

UIDAI was created in 2009 by executive order under the Planning Commission, with the first Aadhaar number generated in 2010 in Nandurbar, Maharashtra. The institutional journey is itself instructive. In its early years the program ran under executive authority, and faced real concerns about privacy and civil liberties. It was placed on a firm statutory footing only with the Aadhaar Act of 2016, whose validity the Supreme Court later upheld. The lesson is that a legal mandate is what ensures a national program can last.

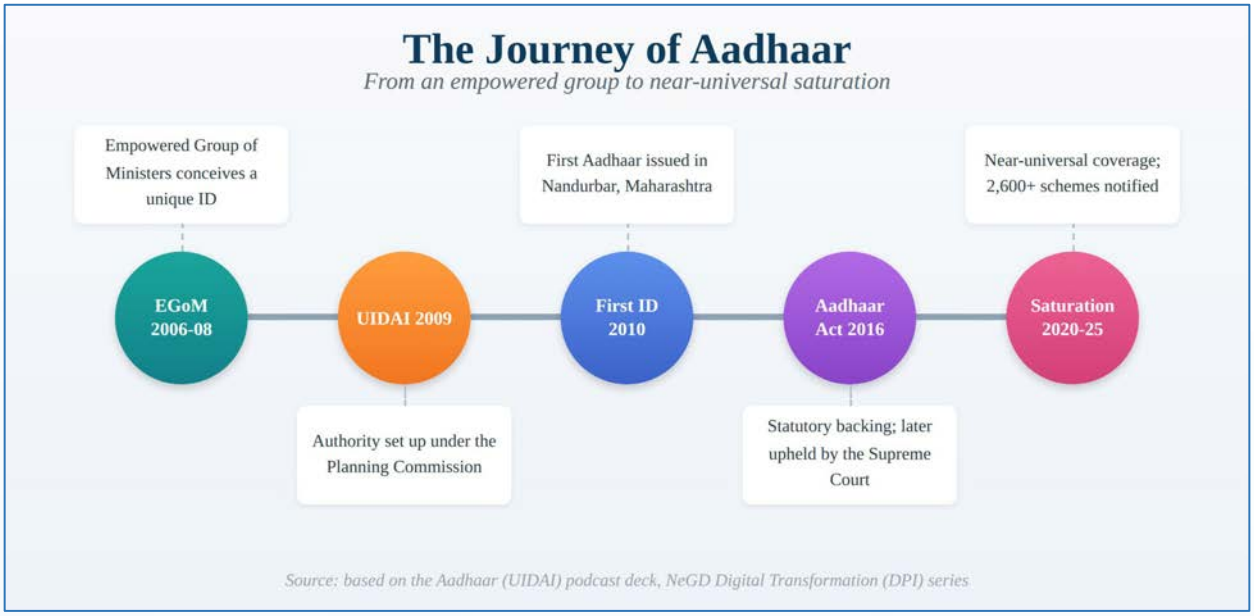



**Figure 2.** *The institutional journey of Aadhaar, from the Empowered Group of Ministers (2005–08) to statutory authority and near-universal saturation (2020–25).*

*Source: based on the Aadhaar (UIDAI) podcast deck, NeGD Digital Transformation (DPI) series.*

Several early decisions proved decisive. Rather than seeking full scheme approval through the slower Expenditure Finance Committee route, the team used the faster Standing Finance Committee mechanism to sanction initial funds, enabling rapid setup while the larger proposal matured, and used existing rate contracts to acquire equipment without fresh tendering. A proof of concept on biometric matching was the first milestone before scaling. The platform was then assembled deliberately: rather than hiring programmers in-house, a professional application development and support agency was engaged through a quality-and-cost-based tender; multiple biometric service providers were engaged so the program never depended on a single vendor; and a contact centre, grievance mechanism and state registrars were established. The recurring lessons are that existing institutional and financial mechanisms can start missions quickly, early proofs of concept build momentum, and prioritising a large program's key components is central to its success.

Crucially, Aadhaar was conceived as a foundational identity rather than a single-purpose card. By providing a verifiable, unique identifier authenticable anytime and anywhere, it became the base for an entire ecosystem, electronic Know Your Customer (e-KYC), e-Sign, DigiLocker, the Aadhaar Enabled Payment System (AePS) and Direct Benefit Transfer, collectively known as the India Stack. By mapping the identifier across bank accounts, benefits could be transferred directly into citizens' accounts, and DBT now spans thousands of schemes. This is the essence of the "think platforms, not projects" philosophy: design for reuse, and downstream innovation follows in domains the original designers never planned for.

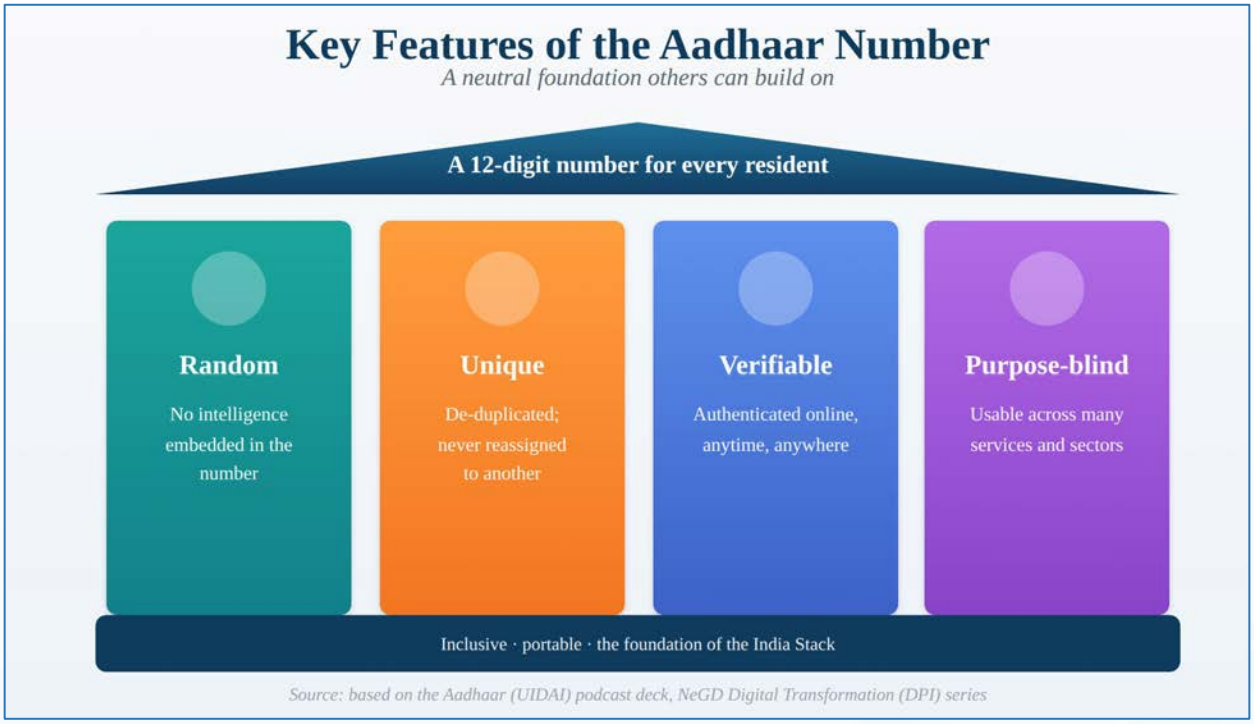



**Figure 3.** *Key features of the Aadhaar number: a 12-digit random, unique, never-reassigned, verifiable and purpose-blind foundational identifier.*

*Source: based on the Aadhaar (UIDAI) podcast deck, NeGD Digital Transformation (DPI) series.*

Two further features speak directly to inclusion and trust. The first is authentication design: Aadhaar supports biometric, one-time-password and demographic matching against the central repository, returning a fast yes-or-no response secured by encryption and a fraud-management system, with newer face authentication offering a contactless method usable on an ordinary smartphone for those who struggle with fingerprint or iris capture. The second is grievance redress: a centralised contact centre on a single national helpline handles enrolment, update, authentication and access queries, with most grievances resolved within seven days across a unified portal, a mobile application, social media and a chatbot, a transparent mechanism that strengthens resident trust.

## 3. The Payments Layer: NPCI and the Unified Payments Interface

If Aadhaar answered the question of identity, the payments layer answered the question of value transfer. The National Payments Corporation of India (NPCI) was incorporated in 2008 by the Reserve Bank of India and the Indian Banks' Association under the Payment and Settlement Systems Act, 2007, as a not-for-profit umbrella body to consolidate fragmented retail payments into a secure, scalable national backbone. NPCI operates India's retail payment rails, UPI, RuPay, IMPS, the Aadhaar Enabled Payment System and the National Automated Clearing House (NACH), as interoperable national platforms.

UPI, launched in 2016, embodied a clear original vision: one application able to access many bank accounts, universal interoperability across banks and merchants, instant round-the-clock payments, and single-click two-factor authentication that was both simple and secure. By using the JAM Trinity (Jan Dhan accounts, Aadhaar identity and mobile connectivity) it reached rural and urban users alike, and has become a global reference point for real-time retail payments.

NPCI's infrastructure also supports inclusive welfare delivery. The National Automated Clearing House is the primary platform for crediting Direct Benefit Transfer (DBT) payments into beneficiary accounts, handling bulk flows of subsidies, pensions and wages, with last-mile withdrawal through the Aadhaar Enabled Payment System, business correspondents, ATMs and bank branches. Reliable DBT infrastructure reduced leakage and built the public trust that later powered mass UPI adoption. Notably, NPCI was set up not as a profit-seeking firm but as a not-for-profit umbrella body owned by a broad group of banks, with the Reserve Bank providing supervision. This public-interest ownership is part of why UPI could become a common rail rather than a proprietary product, and why competing applications work on it without disadvantage. The lesson for auditors and policymakers is that an open, interoperable payments rail compounds in value: each new use case increases the utility of every other.

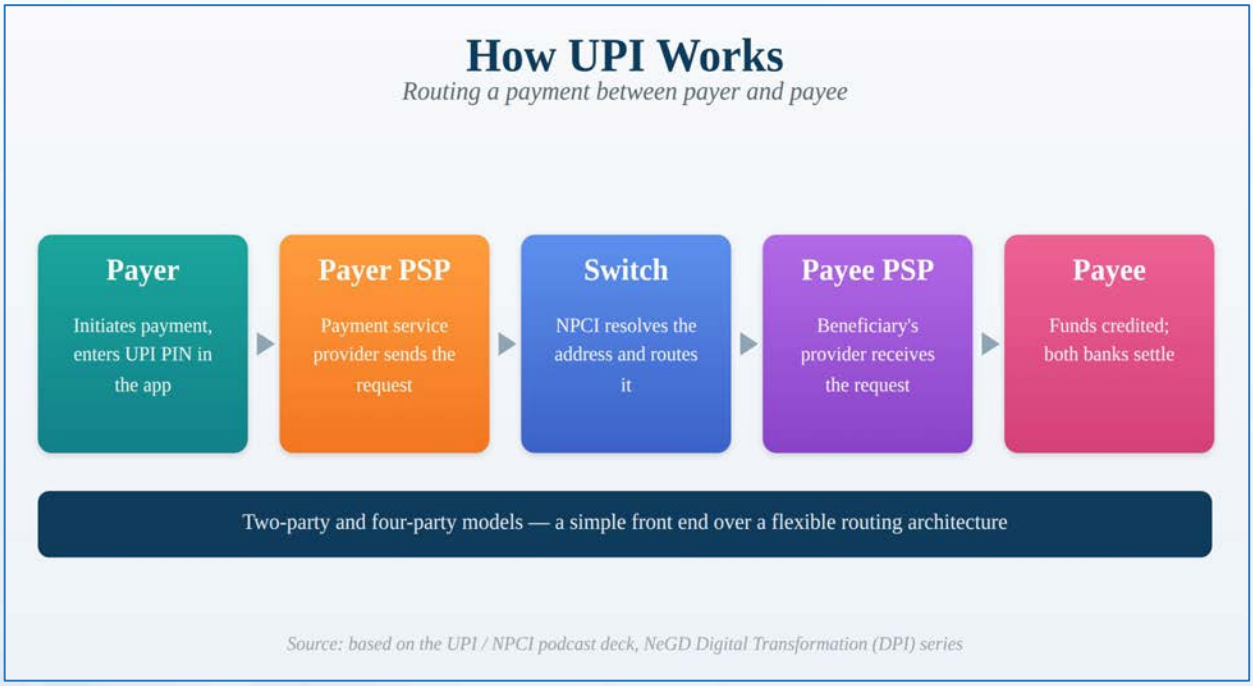



**Figure 4.** *The Unified Payments Interface architecture, showing the two-party and four-party models that route a payment between payer and payee through their banks and payment service providers.*

*Source: based on the UPI / NPCI podcast deck, NeGD Digital Transformation (DPI) series.*

## 4. The Finance and Inclusion Layer: PFMS and PMJDY

Two platforms connect the foundational rails to the machinery of the state. The Public Financial Management System (PFMS), developed by the Office of the Controller General of Accounts with

the National Informatics Centre, tracks the flow of public funds in real time, from sanction to final expenditure. It was born from a concrete need: fragmented, delayed fund flows, no real-time visibility into disbursement, manual reconciliation and weak audit trails. Beginning in 2009 as a tool for monitoring plan schemes, PFMS grew into the backbone for DBT and government accounting, integrated with the central bank's e-Kuber system and hundreds of financial institutions, scaling from a few crore payments a year to hundreds of crores.

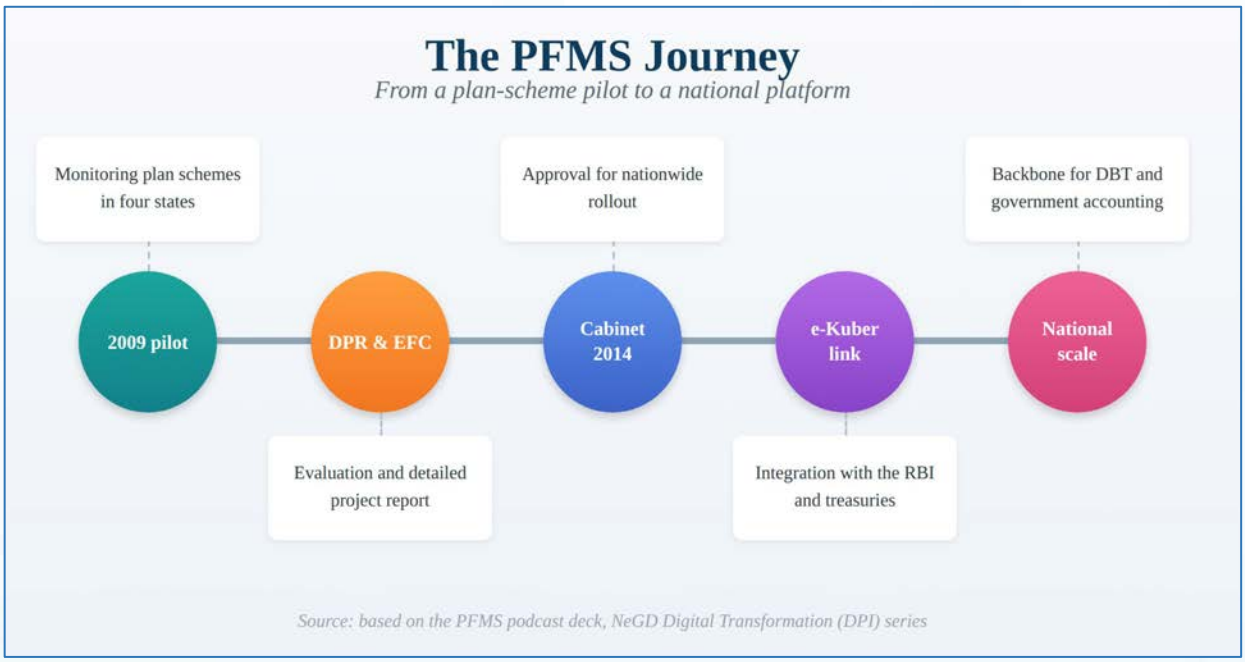



**Figure 5.** *The PFMS journey, from a four-state pilot (2008–09) through Cabinet approval (2014) to a nationwide platform with successive modules for treasury integration, e-Kuber and the Single Nodal Agency system.*

*Source: based on the PFMS podcast deck, NeGD Digital Transformation (DPI) series.*

The Pradhan Mantri Jan-Dhan Yojana (PMJDY), launched in 2014 as a national mission on financial inclusion, supplied the demand side, the accounts themselves. Around 2013–14, only about 35 percent of Indian adults held a bank account, and earlier inclusion drives had fallen short by targeting villages rather than every household. PMJDY took a household-focused approach, opening zero-balance accounts with a debit card, accident insurance and an overdraft facility, and explicitly laying the foundation for the JAM Trinity and the DBT reforms that followed.

The complementarity between PFMS and PMJDY is the point. PFMS gave the state real-time visibility over the flow of public money, PMJDY ensured an account to receive it at the last mile, and the NPCI rails, anchored on Aadhaar, moved it there reliably. The principle is that a payment rail is only as inclusive as the population of accounts it can reach, and a fund-flow system only as trustworthy as the audit trail it leaves behind.

## 5. The Service-Delivery Layer: GeM, GSTN, ABDM and eSanjeevani

Atop the foundational and finance layers sit sector platforms applying DPI principles to specific domains. The Government e-Marketplace (GeM), launched in 2016 and enabled by an amendment to the General Financial Rules, replaced a fragmented, manual, opaque procurement landscape with a single online marketplace built on efficiency, transparency and inclusiveness; structured as a self-sustaining entity, it lowered entry barriers for small businesses and made procurement data available for audit. The Goods and Services Tax Network (GSTN) digitised indirect-tax administration following GST, a value-added, destination-based tax that eliminated the cascading "tax on tax". GSTN handles registration, returns, payments, inter-state settlement and e-invoicing at national scale, showing how a shared backbone can unify a previously state-by-state system.

In health, two complementary efforts stand out. The Ayushman Bharat Digital Mission (ABDM), launched in 2021, builds the national digital health infrastructure, the ABHA health identifier, provider and facility registries, and a consent framework, to make health records interoperable while protecting citizen autonomy. Alongside it, eSanjeevani, developed by the Ministry of Health and Family Welfare through Centre for Development of Advanced Computing (C-DAC), Mohali, brought specialist care to remote areas through two modes: a direct doctor-to-patient OPD service, and a hub-and-spoke model connecting Health and Wellness Centres to doctors at district hospitals. Built on availability, accessibility, affordability and quality, it operates free of charge and has scaled to a presence in all districts, with over 48 crore consultations delivered.

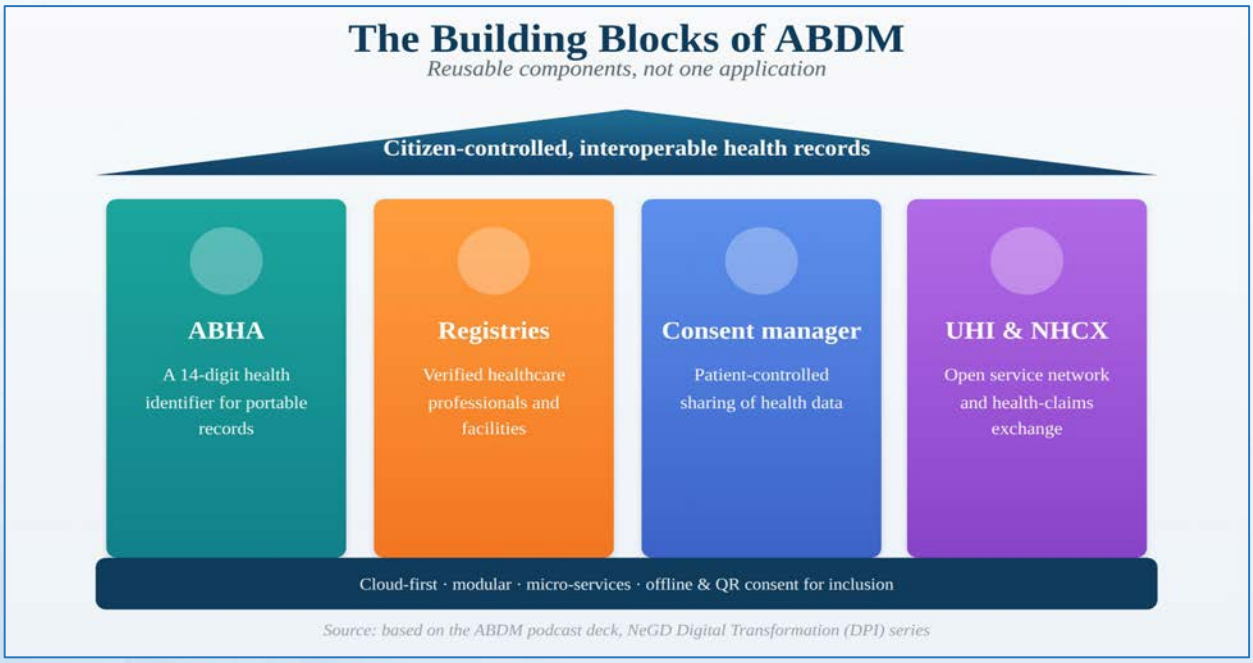



**Figure 6.** *The technology architecture of the Ayushman Bharat Digital Mission, built on DPI principles: cloud-based, multi-tenant, modular and micro-services-based, with offline and QR-based consent solutions for inclusion.*

*Source: based on the ABDM podcast deck, NeGD Digital Transformation (DPI) series.*

The eSanjeevani experience is especially instructive on how a public platform can be built at speed without abandoning propriety. Where a large platform would ordinarily proceed through a full request-for-proposal cycle, the urgency of the COVID-19 pandemic demanded rapid deployment, made possible while preserving accountability by two conditions. First, the Telemedicine Practice Guidelines of March 2020 supplied the legal framework to scale teleconsultation nationally. Second, because the platform was already being developed by a government research institution under a government-to-government model, it could be deployed directly. The General Financial Rules allow nomination-based engagement of a competent public-sector institution in an emergency, provided the ministry documents the context and the institution's capabilities. Transparency is maintained through inter-ministerial approvals and post-facto review. Inclusion was designed in rather than bolted on: the service is free, multilingual and simple to register for, and saw a majority of consultations handled by women doctors.

## 6. Procurement, Security and Continuity: The Less Visible Foundations

Behind every visible platform lies a less visible discipline of procurement, security and institutional continuity that is of particular interest to auditors. On procurement, the experience of some of the country's largest technology tenders points to clear principles: allow bidders adequate time; give clear answers in clarification rounds; ensure transparent evaluation with published marking parameters; keep eligibility criteria minimal and objective; and include external subject experts on evaluation committees. On security, a platform handling personal data and real-time transactions at population scale builds in disaster recovery and business continuity, round-the-clock monitoring and audit trails, role-based access control and regular vulnerability assessments, the foundation of the citizen trust on which adoption depends.

## 7. Cross-Cutting Design Principles

Read together, these platforms reveal a consistent design grammar. First, foundational layers were built deliberately for reuse: identity, payments and data exchange were treated as public utilities on which both government and private innovators could build. Second, the state used the institutional and financial mechanisms it already possessed, including government research bodies, faster financial-approval routes, semi-government agencies for tendering, existing rate contracts, to move from concept to deployment without waiting for perfect conditions. Third, equity and openness were design parameters rather than afterthoughts: multilingual interfaces, last-mile access, zero-cost services, and open standards that prevented vendor lock-in. Fourth, accountability was engineered in through service-level agreements, milestone payments, audit trails and grievance redress. A fifth, easily overlooked principle is the sequencing of trust. Aadhaar earned trust by making identity verifiable, and DBT by delivering entitlements reliably. Only on that foundation did mass voluntary adoption of UPI become possible. Inclusive

governance is as much about building legitimacy in the right order as about building the right technology.

## 8. From Digital Rails to Intelligent Rails: Scale and the Artificial Intelligence (AI) Layer

Eleven years into the Digital India programme, the scale these platforms have reached is itself the strongest evidence of inclusion. As of the eleven-year milestone in mid-2026, Aadhaar had crossed 144 crore (1.44 Billion) enrolments; the Unified Payments Interface handled 24,162 crore (241.62 billion) transactions in 2025-26, up from just 2 crore (20 Million) in 2016-17, and now handles close to half the world's real-time digital payments; DigiLocker served over 70 crore (700 Million) users with more than 850 crore (8.5 Billion) documents issued; and Direct Benefit Transfer had delivered over ₹51 lakh crore ($532.9 billion) to some 176 crore cumulative beneficiaries, saving an estimated ₹3.5 lakh crore ($36.57 billion) by plugging leakages. The JAM Trinity that supports this, Jan Dhan accounts up from 14.72 crore ($1.54 million) in 2015 to 57.78 crore ($6.11 million), near-universal Aadhaar coverage, and mobile and internet access reaching well over a hundred crore people, turned near-zero access into population-wide reach in about a decade.

India's next leap is to layer artificial intelligence onto this proven base. The trusted rails of Aadhaar, UPI and DigiLocker are being made more inclusive, multilingual and intelligent, through translation across dozens of Indian languages, conversational citizen assistance, AI-assisted triage in telemedicine and advisories for farmers. This is the aim of the IndiaAI Mission, a full-stack national effort spanning shared compute, indigenous foundation models, datasets, skilling and a Safe and Trusted AI pillar, complemented by national AI governance guidelines built around trust, fairness, accountability and safety. India's DPI has also become a global public good: through India Stack Global, more than fifteen building blocks have been shared worldwide, UPI has gone live in several partner countries, and a growing number of nations have signed agreements to adopt India Stack components. For Supreme Audit Institutions, the arrival of AI on public rails widens the audit agenda to the fairness, explainability and data protection of algorithmic systems at scale, while the modular, open-standard nature of these rails makes the model adaptable to very different national scales.

## 9. Discussion: Implications for Audit and Inclusive Governance

For Supreme Audit Institutions, the shift from projects to platforms changes the nature of the audit question. When the unit of analysis is a single application, audit can focus on whether it met its objectives within budget. When the unit is shared public infrastructure that thousands of services depend upon, the questions become systemic: Is the platform governed by a clear legal mandate and institutional accountability? Are mission-critical functions retained under public control while the rest is outsourced under enforceable contracts? Is the system secure and

resilient, with disaster recovery, continuity planning and monitored access? And, most importantly for inclusive governance, does the design actively reach the excluded, or inadvertently create new forms of digital exclusion?

India's experience suggests that DPI can be a powerful equaliser, but it also surfaces risks that auditors must scrutinise: the protection of personal data at population scale, the auditability of algorithmic and biometric processes, dependence on a small number of technology partners, and the durability of institutions beyond the tenure of their founders. These are not arguments against DPI; they are the agenda for auditing it well. The transferability of the model is real but conditional. Each jurisdiction must adapt it to its own legal traditions, state capacity and social context. What travels is not the specific software but the philosophy: design foundational platforms on open standards, embed inclusion and accountability from the outset, and govern them as enduring public infrastructure rather than transient projects.

In conclusion, India's Digital Public Infrastructure is a deliberate answer to a long-standing governance problem: how to recognise, pay, serve and account for a billion people inclusively. By building layered, interoperable platforms, from Aadhaar's identity to UPI's payments, from PFMS and PMJDY's financial plumbing to the service platforms of procurement, tax and health, now with AI layered on top, the country turned exclusion into access at scale. For the international audit community, the lesson is that the most important public systems of this era are no longer discrete applications but shared infrastructures, and that auditing them well, for security, durability and above all inclusion, is among the defining responsibilities of modern public-sector oversight.

## References

This article draws on the Digital Transformation (DPI) Podcast series produced by the National e-Governance Division (NeGD), which features conversations with the senior officials associated with Aadhaar, UPI, PFMS, PMJDY, GeM, GSTN, ABDM and eSanjeevani.

Population-scale figures cited in this article are drawn from official Government of India sources, principally the Press Information Bureau (PIB) "Digital India: 11 Years" fact sheet and related MeitY, UIDAI, NPCI, GSTN and ministry releases of June–July 2026.

# How Digital Systems Become Public Infrastructure: DPI Transformability and the Institutional Conversion of Digital Public Infrastructure


## Kentaro Saito

Board of Audit of Japan





## Abstract

Digital Public Infrastructure (DPI) is attracting attention as a shared and interoperable digital foundation for digital ID, payments, data exchange and other functions (OECD, 2024; UNDP, 2023; World Bank, 2025). However, existing discussions on DPI tend to focus heavily on 'what functions it possesses,' and have not sufficiently theorised the conditions under which existing administrative systems, market infrastructures and technical systems can be transformed into public DPI.

This article reframes DPI not merely as a collection of digital building blocks, but as an institutional and technical infrastructure that can be transformed into social common capital within a digital society. To this end, it introduces the concept of 'DPI Transformability'. DPI Transformability refers to the institutional, technical and governance capacity to reorient existing administrative and market infrastructures, or newly designed digital infrastructures, towards public value, interoperability, inclusivity, accountability, redress and complementary investment.

As one such attempt, this article compares four case studies from Estonia, India, Brazil and Germany. Estonia demonstrates a model of administrative interoperability characterised by a high degree of institutional and technical coherence, centred on electronic ID, electronic signatures and X-Road (Kalvet, 2012; Jackson, Dreyling and Pappel, 2021; Hardy, 2024). India, through Aadhaar, Unified Payment Interface (UPI), DigiLocker and other systems, demonstrates the potential of a modular DPI in a society with a massive population, alongside the risks of exclusion, privacy breaches and centralisation (Rao and Nair, 2019; Anand, 2021; Gaur and Eaves, 2025; Chopra, Sidana and Arora, 2025). Brazil is an ongoing example of a payment-led transition to DPI, raising the question of whether the public payment rail centred on Pix can be connected to gov.br and Conecta gov.br. Germany, whilst possessing high general administrative capacity and a mature legal system, is positioned as a case of constraint where 'Origin Fit' and

'Transforming Capacity' for DPI remain at a low to medium level due to existing registers, paper-based administrative practices, IT systems decentralised across federal states and municipalities, and complex delineations of responsibility (Botta, 2022; Kuhlmann and Heuberger, 2023; Nagel, 2025).

The central thesis of this article is that DPI is not a static technical object to be introduced, but rather an institutional transformation process that must be governed. Its public value depends on the extent to which existing administrative, market, and technological infrastructures can be transformed into social common capital that embodies accountability, interoperability, inclusivity, and the possibility of appeal.

## Keywords

Digital Public Infrastructure, DPI Transformability, social common capital, public value, interoperability, Estonia, India, Brazil, Germany.

## 1. Introduction

Digital Public Infrastructure (DPI) refers to a concept whereby common functions—such as digital ID, digital payments and data exchange—are developed as a shared platform that can be reused by both public and private services (OECD, 2024; UNDP, 2023; World Bank, 2025).Whereas traditional digitalisation of public administration has involved building separate systems for specific sectors such as taxation, social security, healthcare, licensing and education, DPI is conceived as a cross-cutting infrastructure connecting multiple policy domains and public and private services (Dunleavy et al., 2006; Janowski, 2015).

However, evaluating DPI solely on the basis of functional classifications such as digital ID, payments and data exchange fails to explain why significant differences in inclusivity, trust, reusability, private-sector innovation and administrative efficiency arise among countries with similar functions, or why these functions sometimes become reusable public infrastructure whilst in other cases remain merely fragmented administrative or market systems. Discussions by international organisations and on DPI mapping are useful for determining 'whether DPI exists' or 'which functions it possesses' (UCL Institute for Innovation and Public Purpose, 2025), but they do not adequately capture the dynamic process by which existing administrative systems, market infrastructures and technological systems are transformed into public DPI under what conditions.

The sense of unease from which this article takes its starting point lies precisely in this point. A DPI does not become a public infrastructure at the moment it is introduced. Institutional components such as identity verification, payment processing, registries, document management and data exchange are each shaped by distinct purposes, legal bases, operational practices, data structures, and divisions of responsibility. For these to function as a cross-cutting

public infrastructure, they require not merely connection, but a reorientation towards the public good.

This article addresses the following question: under what conditions can existing administrative systems, market infrastructures and technical systems be transformed into DPI as a form of social common capital?

This article introduces a perspective to DPI research that analyses transformation processes rather than functional classifications. To this end, it proposes the construct of 'DPI Transformability' and presents a framework for the integrated assessment of objectives, legal institutions, technology, data, governance, inclusivity and complementary investment. Furthermore, through a comparison of Estonia, India, Brazil and Germany, this article attempts to examine how the pathways of DPI formation, the agents of transformation and institutional frictions influence public outcomes and patterns of failure.

## 2. The Theory of DPI Transformability

In this article, the process of DPI formation is divided into primary and secondary development. Primary development refers to the stage of constructing institutional, technological and market infrastructure—such as tax identification numbers, population registers, social security registers, interbank settlement systems, administrative databases and private payment networks—formed on the basis of specific original purposes. Secondary development refers to the stage at which the infrastructure formed through primary development is redefined, re-institutionalised and redesigned as cross-sectoral DPI. At this stage, issues such as the expansion of intended uses, the broadening of connecting entities, Application programming Interfaces (APIs) and standard specifications, legal frameworks, supervision, consent, auditing, redress, delineation of responsibility and complementary investment come to the fore.

In this article, I refer to the conditions that enable such a transformation as 'DPI Transformability'. DPI Transformability is the institutional, technical and governance capacity to reorient existing administrative and market infrastructures, or newly designed digital infrastructures, towards public value, interoperability, inclusivity, accountability, redress and complementary investment. However, a high capacity for transformation does not, in itself, guarantee public outcomes. The same institutional and technical capabilities could also be used to reinforce surveillance, exclusion, private monopolies, and state control. Therefore, this article examines not only the extent of the capacity for transformation towards DPI, but also its direction.

| Level of Analysis | Concept | Positioning |
|---|---|---|
| Origin Fit | Whether the objectives, institutions and data structures of the primary infrastructure are suited to DPI transformation | Prerequisites for DPI Transformability |
| Transforming Capacity | Can the system be reoriented towards a public DPI through legal frameworks, standards, APIs, oversight, remedies and operational capabilities? | Core conditions for DPI transformability |
| Public Infrastructure Performance | Will this lead to improved access, reusability, and the formation of an ecosystem? | Outcomes |

Viewing DPI as social common capital also forms the basis of this theory. However, the term 'social common capital' used here must be distinguished from the concept of 'social capital' criticised by Fine. Social common capital refers to the institutional and physical foundations that underpin human life, such as education, healthcare, public administration, finance, and social infrastructure (Uzawa, 2005). In contrast, 'Social Capital' often refers to trust, norms, networks and associational resources; Fine criticised the conceptual expansion of this term and the dilution of its political-economic analysis (Fine, 2001, 2010). This article treats DPI not as 'social capital' but as socio-technical infrastructure that can, under certain conditions, constitute 'social common capital'.

This understanding is further reinforced by research on information infrastructure and theories of public value. Star and Ruhleder viewed infrastructure not merely as a technical artefact, but as a relational entity that functions only when embedded in practices, standards, organisations and user communities (Star and Ruhleder, 1996). Bowker and Star have demonstrated that classifications and standards shape social order, visibility, and exclusion (Bowker and Star, 1999). Moore's theory of public value provides a perspective for evaluating public sector outcomes not merely in terms of efficiency, but in terms of legitimacy, public purpose, and the creation of social value (Moore, 1995). Furthermore, Mazzucato, Eaves, and Vasconcellos argue that the public nature of DPI is shaped by design and governance geared towards public value (Mazzucato, Eaves and Vasconcellos, 2024). Cordella and Bonina also demonstrate that public sector ICT should be evaluated not only on the basis of efficiency but also in terms of public value (Cordella and Bonina, 2012). Furthermore, Ostrom's theory of the commons shows that access rules, monitoring, conflict resolution, participation, and accountability underpin the sustainability of shared resources (Ostrom, 1990).

What is important for this article is not simply applying these arguments to DPI. Rather, it lies in reinterpreting whether DPI possesses public character not merely in terms of ownership entities or technical specifications, but as a question of how classification, standards, remedies, oversight and complementary investment are interconnected. DPI Transformability is not a concept for measuring a single amount of capital, but rather a framework for analysing which institutional and technical connections is established when an existing infrastructure is transformed into a public DPI, and where risks of power, exclusion, abuse and lack of accountability arise.

DPI Transformability comprises the following seven elements.

| Components | Key Questions | Typical Risks | Theoretical Basis |
|---|---|---|---|
| Objective Consistency | Are the original purpose and the purpose following DPI conversion consistent? | Misuse, loss of legitimacy | Theories of public value and social common capital |
| Consistency with the legal system | Is there a basis for consent, purpose limitation, disclosure to third parties and remedies? | Infringement of rights, loss of trust | Theory of public value, theory of governance |
| Technical Interoperability | Are APIs, standards and certification specifications reusable? | Fragmentation, lock-in | Information Infrastructure Research |
| Data Connectivity | Are data quality, correction procedures and identifier management adequate? | False positives, exclusion | Classification and Standardisation Theory |
| Governance Effectiveness | Do supervision, auditing and complaint handling function effectively? | Abuse, lack of accountability | Public Value Theory, Commons Theory |
| Inclusive Design | Are there alternative means, support services and accessibility? | Digital Exclusion | Theory of social common capital, theory of public value |
| Complementary investment capacity | Will business reform, staff development and user support progress? | Low usage, lack of impact | The Theory of Digital Government, the Productivity J-Curve |

Based on this framework, this article distinguishes three pathways for the generation of DPI. The first is 'Legacy-to-DPI'. This refers to the pathway whereby existing administrative registers, tax numbers, social security records, government portals, electronic IDs, and the like are subsequently reoriented towards a cross-sectoral public infrastructure. The second is 'Market-to-DPI'. This refers to the pathway whereby market-based infrastructure—such as interbank

settlements, private-sector identity verification and payment networks—is converted into public infrastructure through regulation, standardisation and the assignment of public purposes. The third is 'DPI-by-Design'. This refers to the pathway whereby functions such as identity verification, payments, document sharing, and data exchange are designed from the outset as reusable public digital infrastructure. However, in real-world cases, these do not appear in their pure forms; rather, multiple pathways often overlap.

The comparison below focuses on three key points: origin of creation, the complementarity of legal frameworks and technology, and complementary investments. The origin of creation determines the pathways to DPI transformation and the patterns of failure. Legal frameworks and technological interoperability are complementary; neither alone is likely to yield public outcomes. Furthermore, DPI does not generate value through digital components alone. It is only through complementary investments—such as administrative reform, improvements in data quality, user support, the development of a private-sector ecosystem, and supervisory capacity—that long-term public outcomes can be achieved (Brynjolfsson, Rock and Syverson, 2021).

## 3. Methodology and Scope

This article is a theory-driven comparative case study. Its aim is to present the construct of 'DPI Transformability' and to examine how it can explain the patterns of success and failure of DPI in different institutional and technological contexts. Consequently, this article does not seek to estimate causal effects through large-scale econometric analysis but rather compares the explanatory power of DPI Transformability through a small number of case studies.

The outcomes observed in this article are organised primarily into three aspects. The first is improved access to public services. The second is enhanced interoperability and reusability. The third is the formation of private sector and civic ecosystems. However, these are not treated as strict quantitative indicators, but rather as analytical focal points for comparing the direction and degree of DPI transformation.

The four case studies were selected not as representative samples of each country's DPI, but as examples illustrating theoretically contrasting transformation pathways. Specifically, Estonia exemplifies a highly 'transformable' model of administrative interoperability; India, a large-scale, modular DPI that has some shortcomings; Brazil, an ongoing 'Market-to-DPI' transition; and Germany, a fragmented 'Legacy-to-DPI' transition. Consequently, this article examines DPI 'transformability' not only as a conceptual framework for explaining successful cases but also as a framework for analysing incomplete, fragmented, and constrained DPI transitions.

The theory presented in this article is not applicable without limitation to all digitalisation policies. Its scope lies within policy domains that seek to transform existing administrative, market, and technological infrastructures into shared digital infrastructures that support public, private, and civic activities through cross-sectoral reuse.

# 4. Comparative Case Analysis

## 4.1 Estonia: A Model of High-Transformability Administrative Interoperability

Estonia is regarded as a case study demonstrating high DPI transformability. At its core are the electronic ID, electronic signatures, and X-Road. Since 2001, X-Road has formed the core of Estonia's data exchange architecture (Jackson, Dreyling and Pappel, 2021). It has also been analysed in the context of interoperability with the Nordic region and digital diplomacy (Hardy, 2024). In terms of institutional specifications, official Estonian documents also describe X-Road as a secure data exchange layer between public and private organisations (e-Estonia, n.d.).

Estonia's transition to a digital public infrastructure (DPI) was initiated by the government and administrative reform bodies responsible for national reconstruction and administrative consolidation. The reconstruction of the state following the collapse of the Soviet Union, limited human and financial resources, the need to improve administrative efficiency, and the digital national strategy served as the driving forces behind the transformation of the existing administrative infrastructure into an interoperable digital infrastructure. Furthermore, it has been noted that innovation through public procurement, the capabilities of local ICT suppliers, the scarcity of legacy infrastructure, and an institutional environment capable of managing technical risks all underpinned the development of Estonia's e-government (Kalvet, 2012). As Margetts and Naumann (2017) demonstrate, Estonia is also a significant case study from the perspective of 'Government as a Platform'.

A distinctive feature of Estonia is that the DPI has developed not as a single, massive database, but as a secure exchange layer connecting decentralised administrative and private-sector databases. This structure enhances technical interoperability, data connectivity, and the effectiveness of governance. Although data from each organisation is held in a decentralised manner, it is exchanged via X-Road with authentication, encryption, logging, and auditability. Consequently, Estonia is a case study in which 'Origin Fit' and 'Transforming Capacity' were strongly integrated from an early stage.

However, Estonia is not a universal model. It is based on certain preconditions, such as its small size, high administrative capacity and social trust, alignment with EU legislation, a long-term digital national strategy, and a scarcity of legacy systems. Consequently, it is not the Estonian system itself that should be generalised, but rather the highly 'Transformable' structure that combines purpose alignment, legal system alignment, technical interoperability and auditability.

## 4.2 India: Large-Scale Modular DPI and Inclusion Risks

India is a prime example of 'DPI-by-Design'. Initiatives such as Aadhaar, UPI and DigiLocker have been rolled out as modules for identity verification, payments and document sharing, thereby expanding financial inclusion and access to services (Rao and Nair, 2019; Anand, 2021; Gaur and

Eaves, 2025; Chopra, Sidana and Arora, 2025). Aadhaar, in particular, as a practice of governance through biometrics, has reshaped identity verification, welfare distribution and access to private-sector services, whilst also presenting institutional challenges concerning access, inclusion, privacy, security and identity management (Rao and Nair, 2019; Anand, 2021). Official documents from the Unique Identification Authority of India (UIDAI) and the NPCI may also be used as supplementary sources for verifying institutional specifications (UIDAI, n.d.; National Payments Corporation of India, n.d.).

India's transition to a Digital Public Infrastructure (DPI) was driven by a public-private hybrid institutional ecosystem comprising the government, UIDAI, NPCI, technocrats and private-sector digital service providers. The driving force behind this was the simultaneous realisation of identity verification, financial inclusion, low-cost payments, social benefits, and the expansion of private-sector services within a society with a massive population.

India's strengths lie in scale and modularity. Aadhaar addresses the challenge of identity verification in a society with a massive population, whilst UPI has enabled low-cost, widespread and instant payments. DigiLocker reduces reliance on paper certificates, and the Account Aggregator promotes consent-based financial data sharing. These initiatives have the potential to contribute significantly to improving access to public services and fostering the development of a private sector ecosystem.

However, India also serves as a case study that most acutely illustrates the tension between the public nature and the productivity of DPI. Regarding Aadhaar, issues such as biometric authentication failures, the exclusion of those who are difficult to identify, barriers to accessing welfare benefits, privacy and the scope of private-sector use have been points of contention. Crucially, these issues are not merely unintended side effects arising incidentally outside the realm of DPI. The more identity verification is integrated across social benefits, finance, telecommunications and private services, the more authentication failures and data errors become not merely inconveniences but potential barriers to access to the essentials of daily life. India therefore serves as a case study demonstrating that, whilst DPI can realise inclusion and innovation on a massive scale, it can also create a crisis of public good where inclusive design and redress mechanisms are weak.

## 4.3 Brazil: An Ongoing Case of Payment-Led DPI Transformation

Brazil, centred on Pix, gov.br and Conecta gov.br, demonstrates a different pattern of DPI transformability. Brazil should be treated not as a fully integrated DPI, but as a case where a 'payment-led DPI transformation' is underway, with Pix as its starting point. The analytical value lies in the ability to observe whether a successful public payment rail remains merely a sector-specific financial infrastructure or is transformed into a broader DPI by being linked to administrative IDs, service portals and administrative data integration.

Pix has rapidly gained widespread adoption as a central bank-led instant payment infrastructure, and its design successes and remaining challenges have been summarised by the IMF (IMF, 2023). Furthermore, regarding the impact of real-time payments on the banking system, Gonzalez, Ma and Zeng (2025) have analysed real-time payment systems, including Pix. In response to the fees and market dominance previously enjoyed by major banks and payment service providers, the central bank utilised its regulatory authority to institutionalise participation and interoperability.

However, Pix on its own cannot be considered a comprehensive DPI. The theoretical focus in Brazil lies in the extent to which Pix—as a public payment rail—can be connected to the gov.br (administrative ID and service portal), as well as to the Conecta gov.br (administrative data integration platform), and transformed into a comprehensive DPI. Conecta gov.br is being rolled out as a national interoperability platform designed to facilitate real-time and secure data exchange between government agencies (GovTech Intelligence Hub, 2025). Furthermore, the OECD has highlighted the importance of institutional coordination and service integration in Brazil's digital government reform (OECD, 2018).

The ongoing friction in Brazil does not lie in the adoption of Pix itself, but rather in how to define the boundaries regarding payment data, identity verification and the integration of administrative data. The central bank plans to improve the Special Return Mechanism to address fraud, extortion and operational failures involving the misuse of Pix, and to strengthen the tracking of illicit funds in MED 2.0 (Banco Central do Brasil, 2025). Consequently, in Brazil, the extent to which Pix's success as a financial infrastructure is integrated with gov.br's identity verification and service portal, and with Conecta gov.br's administrative data exchange, is creating institutional tensions between financial data protection, anti-fraud measures, administrative efficiency and surveillance risks.

## 4.4 Germany: Fragmentation under High Administrative Capacity and Low to Medium Transformability

Germany is treated not as a mature DPI case study, but as a case illustrating the constraints under which components of administrative digitalisation fail to transition into DPI. Germany possesses high general administrative capacity, a mature legal system and fiscal capacity, and is equipped with institutional components such as electronic ID, an administrative portal, the Online Access Act (OZG) and register modernisation. Nevertheless, existing registers, paper-based administrative practices, IT systems decentralised across the federal states and local authorities, and complex delineations of responsibility reduce 'origin fit' from the perspective of DPI transformation. Furthermore, the federal system, legal fragmentation, delays in register modernisation, and inconsistencies in IT standards at the state and local authority levels have led to institutional and organisational fragmentation of 'transforming capacity' (Botta, 2022; Kuhlmann and Heuberger, 2023; Nagel, 2025).

The OZG is a large-scale reform that requires the federal and state governments to advance the digital provision of administrative services. However, due to the broad scope of the services covered and the decentralised implementation responsibilities across the federal, state and local levels, it has been difficult to transform the provision of digital services, register integration, standardisation and data exchange into an integrated DPI. Botta (2022) identifies the challenges facing the digitalisation of German public administration as federalism, legal fragmentation and the modernisation of registers. Kuhlmann and Heuberger (2023) also demonstrate that digital transformation faces constraints at the local level. Furthermore, Nagel (2025) argues that tensions arise between traditional administrative practices and innovation during the implementation of the OZG reforms.

The German case illustrates the limitations of explaining delays in digitalisation solely in terms of constraints on administrative capacity. Rather, the problem lies in the difficulty of reconfiguring existing administrative and digital capabilities into cross-cutting public infrastructure. A mature legal system and abundant administrative resources do not, in themselves, generate public connectivity. If existing registers and administrative practices are not suited to the transition to DPI, and if standards, registers, demarcation of responsibilities, implementing bodies and local administrative practices remain fragmented, the transition to DPI will be delayed. Germany therefore serves as a case study illustrating that high general administrative capacity can coexist with low to moderate DPI transformability.

Thus, Germany illustrates a fragmented 'Legacy-to-DPI' pathway. Whilst administrative portals, electronic IDs and the modernisation of registers exist as policy components, they have not yet been sufficiently transformed into a coherent, reusable, and cross-sectoral public infrastructure.

## 5. Cross-comparison and Examination of Propositions

Comparing the four case studies from the perspective of DPI transformability, the findings can be summarised as follows.

| Perspective | Estonia | India | Brazil | Germany |
|---|---|---|---|---|
| Generation Path | Legacy-to-DPI + DPI-by-Design | Legacy-to-DPI + DPI-by-Design | Market-to-DPI | Legacy-to-DPI (unfinished) |
| Transition Stage | High Transformability | High scalability, but a point of contention | In progress | Low to medium transformability |
| Main drivers of transformation | Government and public administration reform bodies, local ICT providers | Government, UIDAI, NPCI, technocrats, private-sector ecosystem | Central Bank, Federal Government Digital Division | Federal, state and local authorities; administrative practitioners |

| Perspective | Estonia | India | Brazil | Germany |
|---|---|---|---|---|
| Main Obstacles | Cyber dependency, scalability constraints | Risk of exclusion | Fraud, financial data protection, integration with public administration | Federalism, legal fragmentation, register modernisation, inconsistencies in IT standards |
| Strict requirements | Legal framework, technical interoperability, auditability | Scale, modularity, ecosystem development | Settlement interoperability, regulatory capacity | General administrative capacity, legal framework, fiscal capacity |
| Weak conditions | Scalability | Inclusivity and Redress | Comprehensive connectivity | Origin Fit, Transforming Capacity and integration of registers and standards with DPI |

Looking at the outcome variables, in Estonia, primary fit and transforming capacity are relatively strongly linked, and improvements in access, reusability and ecosystem formation are evident in a well-balanced manner. In India, whilst improved access and ecosystem formation have progressed rapidly due to technical interoperability and scale, negative outcomes such as authentication failures and exclusion have also arisen. In Brazil, interoperability and financial inclusion are strongly evident in Pix; however, unless connectivity with gov.br and Conecta gov.br progresses, outcomes will be skewed towards the payments sector. In Germany, despite the presence of general administrative capacity and institutional components, the initial suitability of existing registers and administrative practices for DPI is low; furthermore, fragmentation in standards, implementation responsibilities and data integration constrains the transition to reusable, cross-sectoral public infrastructure.

A comparison of the four case studies demonstrates that DPI transformability is not solely a function of administrative capacity. It depends on whether institutional authority, legal basis, technical standards, registers and data infrastructure, accountability, and complementary investments are aligned towards achieving outcomes as public infrastructure.

This comparison reinforces the three main arguments of this article. Firstly, the origin of creation determines the transformation pathway and the patterns of failure. In Estonia, the administrative interoperability model; in India, the modular DPI; in Brazil, the payment-led DPI; and in Germany, the incomplete transformation of legacy administration—each gives rise to distinct patterns of failure. Secondly, legal frameworks and technical interoperability are complementary. Germany demonstrates that even with a mature legal framework, DPI outcomes remain limited if standards, registers and implementation responsibilities are

fragmented. Thirdly, public value depends on complementary institutional investment. Estonia's public procurement and ICT supply capacity, India's private-sector apps and financial ecosystem, Brazil's complementary investment in payment systems, and Germany's delays in register modernisation and standardisation demonstrate that DPI outcomes are determined not merely by technological adoption but by such complementary investments. However, in the case of Brazil, the success of Pix cannot be equated with a DPI transformation in the broad sense. Rather, this article focuses on the tension arising from the fact that such an equivalence has not yet been established. Furthermore, it is important to note in this comparison that Germany is not a case of 'capacity deficiency'. Rather, the higher the general administrative capacity, the stronger the tendency to maintain existing institutions, which can sometimes make a reorientation towards DPI difficult.

## 6. Policy Implications and Limitations

The comparison presented in this article demonstrates that DPI policy must be designed as a process of transformation rather than the mere introduction of a function. It is not sufficient merely to assemble components such as digital ID, payment systems, data exchange, administrative portals and the modernisation of registers; it is necessary to assess their origins, the institutional frictions they entail, and the complementary investments required to reorient them towards public connectivity. The evaluation of DPI must also go beyond short-term cost-effectiveness to include business process reform, human resource development, data standardisation, user support, private-sector service development, and supervisory capacity. Ultimately, DPI should not be evaluated according to the dichotomy of government versus private ownership, but rather on the basis of public purpose, conditions of access, oversight, redress, transparency, participation and competitive neutrality (Fine, 2001, 2010; Ostrom, 1990; Uzawa, 2005).

This article also has its limitations. Firstly, this article is a theory-building comparative case study and does not estimate the causal effects of DPI transformability through large-scale econometric analysis. Secondly, all four case studies are countries with a certain level of institutional capacity; they do not cover cases where state capacity itself is extremely low, nor do they deal with explicit surveillance-type DPIs. Thirdly, whilst this article adopts a country-level comparison, the actual functions of a DPI differ depending on the module, such as ID, payments, documentation, data exchange, and consent management.

Furthermore, DPI Transformability is not a fully developed measurement indicator. Whilst this article presents it as an analytical concept for comparing DPI transformation, determining how to measure its individual elements and which thresholds to use to classify Transformability as high, medium or low is left to future empirical research. For example, 'Origin Fit' is difficult to measure based on institutional documents alone, as it depends on the actual structure of the register, administrative practices, data correction procedures, and the discretion of frontline staff. Consequently, future comparisons must encompass not only institutional design but also

the implementation process. Indeed, the aim of this article is not to view the situation through a binary lens of 'DPI implemented' versus 'DPI not implemented', but rather to enable the analysis of discrepancies between institutional origins, transformability and outcomes as public infrastructure.

## 7. Conclusion

This article has redefined DPI not as a set of functions such as digital ID, payments and data exchange, but as an institutional and technological foundation that can be transformed into social common capital within a digital society. On this basis, I have proposed 'DPI Transformability' as a concept to explain the process by which existing administrative systems, market infrastructures and technological systems are transformed into DPI.

A comparison of Estonia, India, Brazil and Germany demonstrates that the public value of DPI depends not on the presence or absence of specific functions, but on the direction in which existing infrastructure is transformed, who drives this transformation, and what frictions are managed in the process. Estonia illustrates that DPI can function as interoperable social common capital through high levels of institutional and technical connectivity, public procurement and local ICT supply capacity. India demonstrates that whilst DPI promotes inclusion and innovation in a society with a vast population, it also gives rise to challenges to the public good, such as authentication failures, exclusion, privacy concerns and centralisation. Brazil shows that the public payment rail 'Pix' has the potential to transform the market infrastructure into DPI; however, without connectivity to 'gov.br' and 'Conecta gov.br', it remains merely a payment DPI. Germany demonstrates that, even with high general administrative capacity and a mature legal system, DPI transformability is constrained by existing registers, paper-based administrative practices, federalism, legal fragmentation and inconsistencies in IT standards.

DPI is not a static technical entity to be introduced, but rather an institutional transformation process that must be governed. Its public value depends heavily on whether existing administrative, market, and technological infrastructures can be transformed into social common capital that is accountable, interoperable, inclusive, and open to appeal. DPI research must now move beyond the stage of asking 'whether' DPI exists, to the stage of asking 'how, in what direction, and by whom it will be transformed into social common capital'.

## References

Anand, N. (2021) 'New Principles for Governing Aadhaar: Improving Access and Inclusion, Privacy, Security, and Identity Management', *Journal of Science Policy & Governance*, 18(1). doi: 10.38126/JSPG180101.

Banco Central do Brasil (2025) *Pix Forum Discusses Improvements to the BCB's Instant Payment System*. Brasília: Banco Central do Brasil. Available at: https://www.bcb.gov.br/en/pressdetail/2589/nota (Accessed: 16 June 2026).

Botta, J. (2022) 'Federalism, Legal Fragmentation and Register Modernisation: Challenges for the Digital Transformation of Public Administration in Germany', *CERIDAP*, 4, pp. 109–133. doi: 10.13130/2723-9195/2022-4-43.

Bowker, G.C. and Star, S.L. (1999) **Sorting Things Out: Classification and Its Consequences**. Cambridge, MA: MIT Press.

Brynjolfsson, E., Rock, D. and Syverson, C. (2021) 'The Productivity J-Curve: How Intangibles Complement General Purpose Technologies', *American Economic Journal: Macroeconomics*, 13(1), pp. 333–372. doi: 10.1257/mac.20180386.

Chopra, K., Sidana, N. and Arora, R. (2025) : 'Digital Public Infrastructure as a Driver of Financial Inclusion in India', *Discover Sustainability*, 7, Article 155. doi: 10.1007/s43621-025-02507-9.

Cordella, A. and Bonina, C.M. (2012) 'A Public Value Perspective for ICT-Enabled Public Sector Reforms: A Theoretical Reflection', *Government Information Quarterly*, 29(4), pp. 512–520. doi: 10.1016/j.giq.2012.03.004.

Dunleavy, P., Margetts, H., Bastow, S. and Tinkler, J. (2006) *Digital Era Governance: IT Corporations, the State, and e-Government*. Oxford: Oxford University Press.

Fine, B. (2001) *Social Capital versus Social Theory: Political Economy and Social Science at the Turn of the Millennium*. London and New York: Routledge.

Fine, B. (2010) *Theories of Social Capital: Researchers Behaving Badly*. London: Pluto Press.

Gaur, R. and Eaves, D. (2025) *The DigiLocker Story: How India is Digitising its Documents*. Case Study No. 4. London: UCL Institute for Innovation and Public Purpose. Available at: https://www.ucl.ac.uk/bartlett/publications/2025/oct/digilocker-story-how-india-digitising-its-documents (Accessed: 16 June 2026).

Gonzalez, R.B., Ma, Y. and Zeng, Y. (2025) *The Effect of Instant Payments on the Banking System*. Working Paper Series, No. 619. Brasília: Banco Central do Brasil. Available at: https://www.bcb.gov.br/content/publicacoes/WorkingPaperSeries/WP619.pdf (Accessed: 16 June 2026).

GovTech Intelligence Hub (2025) *Conecta gov.br: Brazil's National Interoperability Platform for Automated Data Exchange*. Available at: https://www.govtechintelhub.org/case-study-details/conecta-gov.br%3A-brazil%27s-national-interoperability-platform-for-automated-data-exchange/aJYTG0000000Yxl4AE (Accessed: 16 June 2026).

Hardy, A. (2024) 'Estonia's Digital Diplomacy: Nordic Interoperability and the Challenges of Cross-border e-Governance', *Internet Policy Review*, 13(3), pp. 1–31. doi: 10.14763/2024.3.1785.

International Monetary Fund (IMF) (2023) 'Pix: Brazil's Successful Instant Payment System', in *Brazil: Selected Issues*. IMF Country Report No. 23/289. Washington, DC: International Monetary Fund. Available at: https://www.imf.org/en/Publications/CR/Issues/2023/07/31/Brazil-Selected-Issues-536865 (Accessed: 16 June 2026).

Jackson, E.B., Dreyling, R. and Pappel, I. (2021) 'A Historical Analysis on Interoperability in Estonian Data Exchange Architecture: Perspectives from the Past and for the Future', in *Proceedings of the 14th International Conference on Theory and Practice of Electronic Governance (ICEGOV 2021)*, pp. 111–119. doi: 10.1145/3494193.3494209.

Janowski, T. (2015) 'Digital Government Evolution: From Transformation to Contextualisation', *Government Information Quarterly*, 32(3), pp. 221–236. doi: 10.1016/j.giq.2015.07.001.

Kalvet, T. (2012) 'Innovation: A Factor Explaining e-Government Success in Estonia', *Electronic Government, an International Journal*, 9(2), pp. 142–157. doi: 10.1504/EG.2012.046266.

Kuhlmann, S. and Heuberger, M. (2023) 'Digital Transformation Going Local: Implementation, Impacts and Constraints from a German Perspective', *Public Money & Management*, 43(2), pp. 147–155. doi: 10.1080/09540962.2021.1939584.

Margetts, H. and Naumann, A. (2017) *Government as a Platform: What Can Estonia Show the World?* Oxford: Oxford Internet Institute, University of Oxford.

Mazzucato, M., Eaves, D. and Vasconcellos, B. (2024) *Digital Public Infrastructure and Public Value: What is "Public" about DPI?* IIPP Working Paper No. 2024/05. London: UCL Institute for Innovation and Public Purpose. Available at: https://www.ucl.ac.uk/bartlett/publications/2024/mar/digital-public-infrastructure-and-public-value-what-public-about-dpi (Accessed: 16 June 2026).

Moore, M.H. (1995) *Creating Public Value: Strategic Management in Government*. Cambridge, MA: Harvard University Press.

Nagel, M.L. (2025) 'The Challenge of Balancing Innovation and Tradition in the Public Sector: The Role of Street-Level Bureaucrats in Digital Transformation', *Administration & Society*, 57(2), pp. 313–342. doi: 10.1177/00953997241296100.

OECD (2018) *Digital Government Review of Brazil: Towards the Digital Transformation of the Public Sector*. Paris: OECD Publishing. doi: 10.1787/9789264307636-en.

OECD (2024) *Digital Public Infrastructure for Digital Governments*. OECD Public Governance Policy Papers, No. 68. Paris: OECD Publishing. doi: 10.1787/ff525dc8-en.

Ostrom, E. (1990) *Governing the Commons: The Evolution of Institutions for Collective Action*. Cambridge: Cambridge University Press. doi: 10.1017/CBO9780511807763.

Rao, U. and Nair, V. (2019) 'Aadhaar: Governing with Biometrics', **South Asia: Journal of South Asian Studies**, 42(3), pp. 469–481. doi: 10.1080/00856401.2019.1595343.

Star, S.L. and Ruhleder, K. (1996) 'Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces', *Information Systems Research*, 7(1), pp. 111–134. doi: 10.1287/isre.7.1.111.

UCL Institute for Innovation and Public Purpose (2025) *2025 State of Digital Public Infrastructure Report*. London: UCL Institute for Innovation and Public Purpose. Available at: https://dpimap.org/iipp-state-of-dpi-report-2025.pdf (Accessed: 16 June 2026).

UNDP (2023) *The DPI Approach: A Playbook*. New York: United Nations Development Programme. Available at: https://www.undp.org/publications/dpi-approach-playbook (Accessed: 16 June 2026).

Uzawa, H. (2005) *Economic Analysis of Social Common Capital*. Cambridge: Cambridge University Press.

World Bank (2025) *Digital Public Infrastructure and Development: A World Bank Group Approach*. Washington, DC: World Bank. Available at: https://openknowledge.worldbank.org/entities/publication/cca2963e-27bf-4dbb-aa5a-24a0ffc92ed9 (Accessed: 16 June 2026).

Online primary sources and official documentation

e-Estonia (n.d.) *X-Road: Interoperability Services*. Available at: https://e-estonia.com/solutions/interoperability-services/x-road/ (Accessed: 16 June 2026).

National Payments Corporation of India (n.d.) *UPI: Unified Payments Interface*. Available at: https://www.npci.org.in/product/upi (Accessed: 16 June 2026).

UIDAI (n.d.) *Aadhaar Authentication*. Unique Identification Authority of India. Available at: https://uidai.gov.in/en/contact-support/have-any-question/303-faqs/authentication.html (Accessed: 16 June 2026).

# Digital Public Infrastructure as an Enabler of Inclusive Governance: Mechanisms, Evidence, and the Audit Imperative

**Harsha Bhowmick & Abhishek Singh**
India





## Abstract

For decades, governments have struggled to answer a simple question: how do you reach everyone? - including the connected, the educated, the urban, the documented, the undocumented and everyone. Four structural failures have long made this elusive: citizens invisible to the state because they lack legal identity; welfare funds that evaporate in transit through intermediaries; information asymmetries that keep credit and services out of reach for those who need them most; and geographic exclusion that paper-based system has failed to solve. Digital Public Infrastructure or DPI the foundational architecture of identity, payments, and data exchange is the most profound institutional attempt to address all these issues through use of technology for public good.

This paper does not argue that DPI is a silver bullet. It argues something more precise: that DPI may fundamentally alter the conditions under which inclusive governance is possible, but only when it is governed well, designed equitably, and held to account with the same rigour we apply to any major public investment. Drawing on India's experience, global evidence from Brazil, Sub-Saharan Africa, and South-East Asia, and frameworks from the G20, IMF, World Bank, CGAP, GSMA, OECD, IFAD, and INTOSAI WGITA, the paper examines three governance transformation mechanisms, four gaps that DPI cannot fill on its own, and four dimensions across which Supreme Audit Institutions must build assurance capability.

## Keywords

Digital Public Infrastructure, Inclusive Governance, JAM Trinity, India Stack, SAI Audit, Financial Inclusion, Consent Architecture, INTOSAI WGITA, G20, Data Rights

## 1. Introduction: The Governance Problem DPI Addresses

Ask any senior official responsible for welfare delivery what keeps them anxious and you tend to get variations of the same answer: one just cannot reliably get the welfare delivered to intended beneficiaries. Identity is uncertain. Intermediaries leak. Paper trails are vague. And the people who most need the state's welfare - the rural, the poor, the undocumented - are precisely those the system finds hardest to reach.

This is not a new problem. What may be new is the possibility of a structural solution. Digital Public Infrastructure, as defined by the G20's 2023 New Delhi Leaders' Declaration, refers to digital solutions that act as building blocks for service delivery, built on secure, interoperable, federated, platforms. The key distinction from earlier e-governance efforts is architectural: DPI does not simply digitise existing processes, it provides the digital infrastructure which is meant to scale and be accessible to all citizens without any rent.

India's JAM Trinity offers the most documented proof of concept. By linking Jan Dhan accounts, Aadhaar identity, and mobile connectivity, India achieved 80% financial inclusion in six years, a trajectory that the G20 GPFI estimated would have taken 46 years through conventional banking expansion (G20 GPFI, 2023). Subsidy leakage fell from 16% to 9% of social welfare expenditure (IMF, 2024). The Gates Foundation estimates DPI could accelerate GDP growth in low- and middle-income countries by 20 to 33 per cent (Gates Foundation, 2024). These are not technology metrics but governance outcomes.

The purpose of this paper is to move beyond the headline statistics, which are by now well known, to examine what DPI actually does to the architecture of governance, where it falls short, and what it demands of audit institutions that want to provide meaningful accountability assurance on this new class of public infrastructure.

## 2. Conceptual Framework: The Architecture of DPI

It helps to be concrete about what DPI actually is. At its core, DPI is a three-layer architecture where each layer is useful on its own but transformative in combination. The identity layer answers the question: who is this person? The payments layer answers: how do we get value to them? The data exchange layer answers: how do we share what we know about them, with their consent, and with privacy protections built in?

What separates DPI from ordinary digitalisation is a set of design choices that the G20 Task Force (2023) identified as non-negotiable: interoperability across institutions; minimalism in what data

is collected; federation rather than centralisation; privacy by design rather than privacy as an afterthought; and, critically, protocols rather than platforms. This last principle matters enormously. A platform creates dependency on whoever controls it. A protocol, like UPI's payment rails or the Account Aggregator's consent framework, creates shared infrastructure that any participant can build on. The OECD captured the governance implication well: DPI can enable government to function 'as a single coherent system rather than a collection of disconnected organisations' (OECD, 2025). Figure 1 shows how the layers stack.

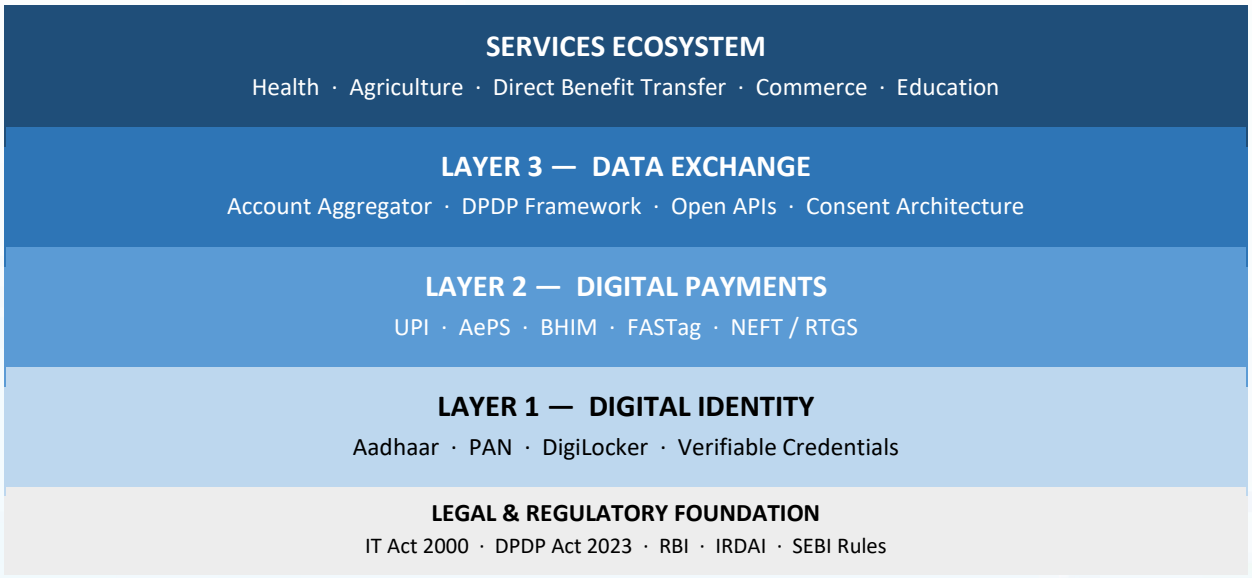



Figure 1: DPI Three-Layer Architecture. Each layer amplifies the value of the layer below; the legal foundation governs the whole stack. Source: G20 Task Force on DPI (2023); authors' adaptation.

## 3. DPI as an Enabler of Inclusive Governance: Three Transformation Mechanisms

Saying DPI 'enables inclusive governance' risks becoming a slogan unless we are specific about how. There are, in the authors' assessment, three distinct mechanisms through which well-designed DPI can shift the governance equation, each compounding the effect of the others.

### 3.1 Mechanism 1 - From Social Entitlement to Enforceable Digital Right

Most welfare states are generous on paper. The right to food, to shelter support, to a pension, these exist in law across much of the developing world. What does not always exist is the operational capacity to honour those rights consistently and without leakage. The gap between the statutory entitlement and what actually reaches the beneficiary has, for generations, been the central governance failure in public welfare.

DPI closes that gap architecturally. When a beneficiary's identity is verified by Aadhaar, her bank account is linked, and her entitlement is credited directly without touching an intermediary, the statutory promise becomes an executable transaction. India's experience illustrates the scale of

the difference: DBT-enabled subsidy payments reduced leakage from roughly 16% to 9% of social welfare expenditure (IMF, 2024). One rupee in every six used to disappear in transit. DPI made that disappearing act structurally harder.

There is also a rights dimension that goes beyond existing beneficiaries. Around 800 million people worldwide still lack any legal identity document (World Bank ID4D, 2024). For these individuals, and they are disproportionately women, migrants, indigenous peoples, and the rural poor, civic invisibility means exclusion not just from welfare but from almost every formal transaction: banking, insurance, business registration, even voting. Open-source DPI platforms like MOSIP, now deployed in the Philippines, Morocco, Ethiopia, and several other countries, can convert that invisibility into legibility at a fraction of the cost of traditional civil registration.

## 3.2 Mechanism 2 - From Intermediary Opacity to Traceable Accountability

The second mechanism may matter even more: DPI restructures accountability. Pre-DPI welfare delivery moved through long chains of intermediaries, district offices, local agents, bank branches, ration shop owners, whose behaviour was largely opaque from any central vantage point. Diversion of funds was often not even detectable until an audit years later, by which point the money was long gone and the beneficiary had simply been told the programme had run dry.

Direct digital payment eliminates the structural opportunity for that kind of diversion. When a transfer is credited to a named, verified bank account, it generates a timestamped record that is retrievable, reconcilable, and auditable. This is not a minor administrative improvement, it is a qualitative change in the accountability architecture of the state. Figure 2 shows what that shift looks like in practice.

| **WITHOUT DPI**<br>Traditional Governance Path | **WITH DPI**<br>DPI-Enabled Governance Path |
|---|---|
| Paper identity; manual verification | **Aadhaar biometric authentication — seconds** |
| Physical office visit required | **Mobile or web interface; zero queues** |
| Intermediary-controlled delivery chain | **Direct citizen-to-government channel** |
| Leakage: ~16% of welfare funds diverted | **Leakage reduced to ~9% through DBT** |
| No reliable audit trail | **Complete timestamped digital audit trail** |
| Grievance redress: slow and opaque | **Grievance redress: traceable, time-bound** |
| 800M+ citizens without legal identity | **DPI-enabled ID restores civic legibility** |
| Accountability diffused across agencies | **Accountability embedded in architecture** |

Figure 2: Traditional versus DPI-Enabled Governance Pathway. The DPI path eliminates intermediaries, compresses processing time, and creates a complete audit trail. Source: Author's analysis; G20 Task Force (2023); IMF (2024).

For SAIs, the implication is direct. The same digital trail that makes governance more accountable also makes it more auditable. Reconciling entitlements against payments, detecting systematic non-delivery, mapping exclusion patterns across geographies and demographic groups, all of this is now technically possible in ways that were simply not feasible in a paper-based system. DPI may turn out to be as important for government auditing as it is for government service delivery.

## 3.3 Mechanism 3 - From Passive Recipients to Empowered Participants

The third mechanism is the most novel and, arguably, the most significant for long-run governance quality. Conventional public administration treats citizens as subjects of data flows, the state and market collect data about people, aggregate it, and act on it, with little transparency and less control for the people concerned. The consent architecture embedded in DPI's data exchange layer turns that relationship around.

India's Account Aggregator (AA) framework is the clearest example. Under the AA model, a small farmer or informal worker can authorise her bank to share her financial history with a lender through a consent-gated API, opening access to credit that traditional underwriting models would have denied her, because she lacks the collateral or credit history those models require. By March 2024, 64 million accounts had been linked through the AA ecosystem (CGAP/RBI, 2024). CGAP has described the potential as a 'UPI-like transformation' in small business credit markets, a significant characterisation from an institution not prone to hyperbole.

The DPDP Act 2023, with Rules notified in November 2025 and a Data Protection Board now constituted, elevates this consent architecture into a framework of legally enforceable rights: the right to access one's own data, to correct it, to withdraw consent, and to seek redress when those rights are violated (MeitY, 2025). Citizens are no longer just the subjects of DPI. They may be becoming its owners. Figure 3 illustrates how these three mechanisms can, when governance holds, create a self-reinforcing cycle.

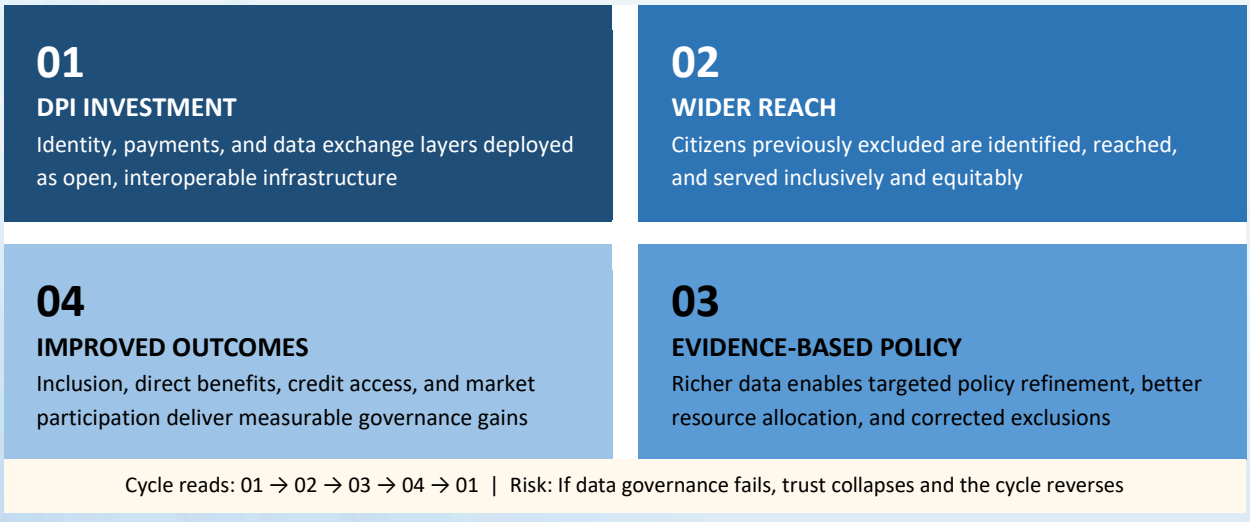



Figure 3: The DPI-Inclusive Governance Virtuous Cycle. Numbers 01-04 indicate the cycle sequence. The cycle is self-reinforcing when governance is sound; self-defeating when data governance fails. Source: Authors' analysis.

## 4. India's Evidence: Governance Outcomes, Not Just Statistics

India's DPI story is by now familiar in outline. What is less often examined is what the numbers actually mean as governance evidence.

The scale is genuinely remarkable: 27.07 billion Aadhaar authentications in 2024-25 (UIDAI, 2025); UPI handling 700 million transactions on peak days, contributing an estimated $16.2 billion to annual GDP (IMF/NPCI, 2024); a Welfare Efficiency Index that improved from 0.32 to 0.91 in the Jan Dhan period (Internal Policy Memo, 2023); and an RBI Financial Inclusion Index of 67 (RBI, 2024) that measures depth of use, not just account ownership. These are extraordinary numbers. But the governance question is: what do they displace?

What they displace is a system in which, by conservative estimates, one rupee in six allocated to welfare never reached its intended beneficiary. That is not primarily a story about venal individuals, it is a story about a system so opaque that diversion was structurally easy and detection was structurally hard. DPI-enabled DBT made diversion structurally harder and detection structurally easier. That is a governance achievement of a fundamentally different kind from, say, hiring more inspectors or introducing stricter penalties.

ONDC adds another dimension worth noting. By establishing an open protocol for digital commerce, ONDC reduced platform commissions from 15-30% to 3-5% and brought 116,000 small sellers into digital markets they had previously been priced out of (Internal Policy Memo, 2023). The Account Aggregator framework has begun doing something similar in credit markets: giving the self-employed, the informally employed, and the micro-entrepreneur the data visibility to access formal credit for the first time. Full compliance with the DPDP Act 2023 governance framework for these data flows is required by May 2027, which should itself be a focus of SAI audit planning.

## 5. Global Evidence and Multilateral Momentum

India's experience is the most extensively documented, but it is not anomalous. Brazil's Pix payment system and open finance framework brought 43 million accounts into the AA-equivalent ecosystem by March 2024 (CGAP, 2024), demonstrating that rapid DPI-enabled financial inclusion is reproducible in different institutional contexts. GSMA's 2025 State of the Industry Report records $2 trillion in annual global mobile money transactions, double the 2021 figure, with Sub-Saharan Africa, where mobile money is often the only DPI payments layer that exists, accounting for the largest share (GSMA, 2025). MOSIP is live or in pilot across seven countries, making open-source DPI a serious development tool, not just a concept.

The multilateral architecture has moved from interest to conviction. The World Bank's ID4D initiative covers 60+ countries (World Bank, 2024). The IMF's analytical work treats DPI as both an inclusion instrument and a macroeconomic productivity driver (IMF, 2024). The ADB estimates a 50% reduction in South Asian government administrative costs from DPI deployment

(ADB, 2025). IFAD is integrating DPI into remittance and rural finance programmes across its portfolio. Under South Africa's 2025 G20 Presidency, the GPFI has pushed the agenda beyond 'getting accounts' to 'using accounts', deepening usage, extending DPI to MSME credit, and embedding interoperability standards across payment systems (South Africa GPFI, 2025).

Perhaps the most significant signal is convergence. The IMF, GSMA, CGAP, OECD, World Bank, ADB, and INTOSAI WGITA are not organisations that typically reach the same conclusion. When they do, and they have, on the potential of DPI, it is worth paying attention.

## 6. Critical Assessment: The Governance Gaps DPI Cannot Fill

Precisely because DPI's potential is real, it is important to be honest about what it cannot do. Infrastructure is not the same as political will. A well-built DPI system can be deployed in the service of exclusion as easily as inclusion, it depends entirely on the institutional choices made around it. Four governance gaps deserve explicit attention, because each requires a governance response rather than a technical fix.

### 6.1 The Last-Mile Gap

DPI reaches a smartphone. It does not, by itself, reach the 70-year-old woman in a remote village whose fingerprints have degraded, who has never used a mobile application, and who has spent her life navigating a state that routinely failed to see her. GSMA documents that 1.5 billion people globally still lack any official identity document (GSMA, 2025). For many of them, the preconditions for DPI, a device, a SIM, a bank account, a biometric enrolment, simply do not yet exist. CGAP's analysis is precise on this point: the barriers are not primarily financial, they are structural, social, and geographic, and they require parallel investment that no DPI rollout can substitute for (CGAP, 2025).

### 6.2 The Accountability Diffusion Gap

One of the less-discussed risks of multi-stakeholder DPI is that it can make accountability harder rather than easier. When an identity authority, a payment network, three commercial banks, a fintech intermediary, and a line ministry are all involved in delivering a single benefit, and something goes wrong, the question of who is responsible, and who the citizen goes to for redress, can become genuinely unanswerable. The DPDP Act creates a Data Protection Board for data rights grievances. Indian Computer Emergency Response Team (CERT-In) handles cybersecurity. But there is, as yet, no institutional home for the DPI service failure that leaves a welfare beneficiary simply unable to access what she is legally owed. Cross-cutting SAI performance audits may be the only accountability mechanism with the mandate to follow that failure across agency boundaries.

## 6.3 The Data Power Asymmetry

There is an uncomfortable possibility at the heart of DPI's data exchange layer: the consent architecture that empowers citizens in theory may, in practice, empower the institutions that design the consent flows. Consent forms written in technical language, consent mechanisms accessible only via apps requiring digital literacy, consent that is technically revocable but practically difficult to withdraw, these are not hypothetical risks. They are documented patterns in consent-based data systems globally. The DPDP Act 2023 and the AA framework are genuine attempts to address this asymmetry, but their effectiveness will ultimately depend on the enforcement capacity of the Data Protection Board, the legal quality of judicial review when data rights are contested, and, critically, the accessibility of consent mechanisms to the least-educated users. SAI compliance audits of DPDP and other such relevant act's implementation should be on every SAI's agenda.

## 6.4 The Trust Equation

All of the above converges on trust. DPI without citizen trust is infrastructure without users. India's early Aadhaar rollout encountered precisely this problem: documented authentication failure rates among manual labourers whose fingerprints had degraded, among the elderly, and among people in areas with poor biometric sensor quality. These were not edge cases, they were the populations DPI was designed to serve. The failures were largely addressed over time, but not before generating a layer of distrust that still shapes adoption patterns a decade later. The lesson is not that DPI fails in hard cases. It is that trust must be earned through consistent, equitable performance, and that equity audits, specifically designed to detect whether failure rates are systematically concentrated in particular demographic groups, are an essential instrument for catching and correcting these patterns early.

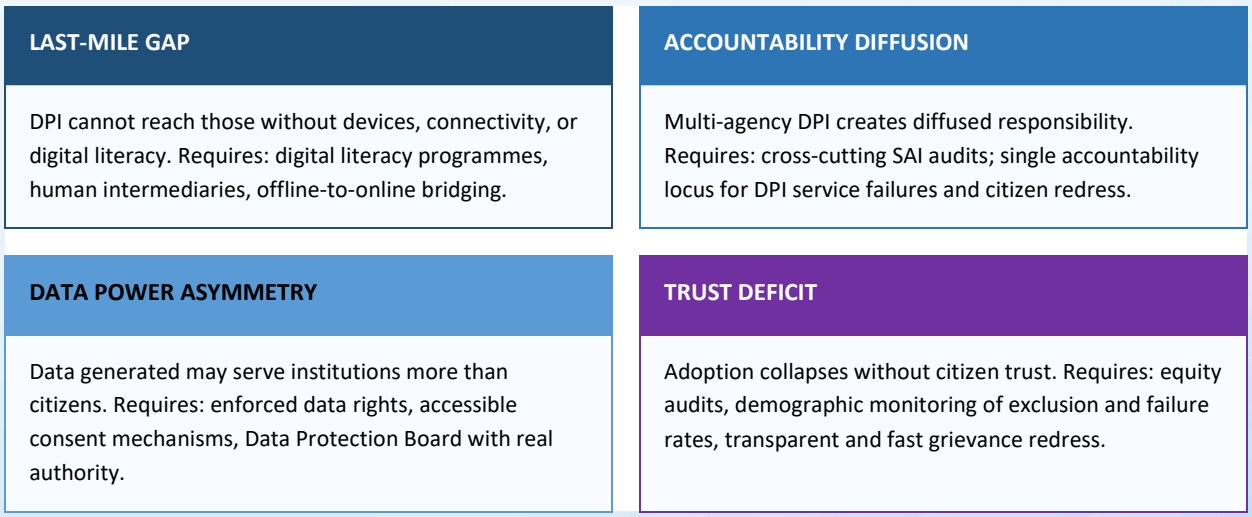



Figure 4: Four Governance Gaps DPI Cannot Fill. Each gap requires a governance response, not a technical upgrade. Source: Authors' analysis.

## 7. The SAI Audit Imperative: Auditing Inclusive Governance through DPI

Supreme Audit Institutions hold a mandate that no other accountability body in the DPI ecosystem can replicate. Data protection authorities focus on privacy. Sector regulators focus on markets. Parliamentary committees focus on policy. Only SAIs have both the independence and the cross-sectoral reach to ask, and credibly answer, whether DPI is actually delivering what it promises across the full range of its governance functions.

In April 2026, CAG India released the Digital Public Infrastructure Audit Guidelines -- the first dedicated, ISSAI-aligned audit framework built specifically for DPI systems, developed for use across INTOSAI regions and drawing on practice from India, Estonia, Singapore, Brazil, and the European Union. The Guidelines integrate ISSAI and GUID standards as the professional audit foundation, the People-Process-Tools & Technology-Data Governance (PPT&D) framework as the analytical lens, the UN Universal DPI Safeguards Framework (2024) as the governance reference, and relevant ISO and sectoral standards as control benchmarks for auditing Digital Public Infrastructure (CAG India, 2026).

What Figure 5 below proposes is that SAIs think about DPI audit not as an IT audit exercise alone, but as four overlapping dimensions of accountability assurance.

| Four-DIMENSION SAI AUDIT FRAMEWORK FOR DPI SYSTEMS | | | |
|---|---|---|---|
| **IT / IS** Audit | **COMPLIANCE** Audit | **PERFORMANCE** Audit | **EQUITY** Audit (Emerging) |
| Access management controls | DPDP Act 2023 / Rules 2025 | Inclusion outcomes vs targets | Data disaggregated by gender |
| Change management processes | DBT leakage detection | Procurement value for money | Regional exclusion mapping |
| Disaster recovery & BCP | Data governance frameworks | Last-mile access metrics | Authorization failure by demographic |
| Incident response & CERT-In | Consent mechanism compliance | User grievance turnaround | Bias detection in design |
| | Vendor contracts & lock-in risk | Financial sustainability of DPI ops | |

Figure 5: Four-Dimension SAI Audit Framework for DPI. Equity Audit is an emerging dimension not yet standard in most SAI methodologies. Source: Authors' analysis; IDI-WGITA Handbook; CAG India, SAI India DPI Audit Guidelines (2026); CAG IS Audit Manual 2024.

Three questions, in particular, stand out as ones that SAIs should ask systematically:

- Does the DPI system produce and publish disaggregated data on authentication failures, exclusion events, and unresolved grievances, broken down by gender, social category, geography, and income level, enabling the state and the SAI to identify who is being systematically left out?

- When a legally entitled beneficiary does not receive her transfer, is there a traceable accountability chain showing at which point in the DPI pipeline the failure occurred, which agency bears responsibility, and what the required redress timeline is?
- Are the consent mechanisms through which citizens share data under the DPDP Act 2023 and the AA framework genuinely accessible to low-literacy, low-connectivity users, or are they, in practice, compliance formalities that create the appearance of consent without its substance?

The DPI Audit Guidelines address this through the audit objective on **Inclusion, Access & Privacy for Citizens**, which tests outreach, consent, accessibility, data minimisation, and citizen rights across the data lifecycle against the **Leave No One Behind** principle and calibrates expectations to the maturity of the DPI ecosystem (CAG India, 2026).

No regulator, data protection board, or parliamentary committee has the institutional position to pursue all three of these questions simultaneously. SAIs do.

## 8. Conclusion: From Infrastructure to Governance Commitment

DPI is a precondition for inclusive governance, a remarkable and historically unprecedented one, but it is not the same thing as inclusive governance. The state now has technical capabilities it never previously possessed: the ability to verify identity in milliseconds, to transfer resources directly without leakage, to generate a full digital record of every transaction, and to enable citizens to share their own data on their own terms. Whether those capabilities are exercised in the interest of all citizens, or primarily in the interest of those who are already well-served, is a governance choice, not a technical one.

The three mechanisms examined in this paper, converting statutory entitlements into executable digital rights, replacing intermediary opacity with traceable accountability, and repositioning citizens from passive recipients to data sovereigns, are each genuine, demonstrated, and reproducible. None of them is automatic. Each depends on institutions keeping their commitments: a legal framework that enforces data rights (DPDP Act 2023), a regulatory architecture that maintains interoperability, a political commitment to zero transaction costs for low-income users (UPI's zero MDR policy), and a civil society with the capacity to contest exclusions when they happen.

The four governance gaps identified in Section 6 are not objections to DPI. They are the agenda for its next phase, the harder, slower, more politically contested work of governing DPI inclusivity once it is built. That work will require investments in human intermediaries for the last mile, in legal enforcement of data rights, in institutional coordination across fragmented accountability systems, and in the kind of sustained political attention that outlasts the excitement of a new technology's launch.

SAIs have a distinctive role in that next phase. Not just auditing DPI systems, though that is necessary, but auditing whether DPI is delivering what inclusive governance actually demands. The INTOSAI WGITA 2026-28 Work Plan and the DPI Audit Guideline 2026 provide the methodological foundation. What remains is the institutional commitment to use them, across all the dimensions of Figure 5, and with the organising question firmly in view: not 'Is the DPI system working?' but 'Is it working for everyone?'

## References


ADB. (2025). ADB Digital Policy Report 2025: South Asia digital transformation. Asian Development Bank.

Bill & Melinda Gates Foundation. (2024). Our work in digital public infrastructure. https://www.gatesfoundation.org

CAG India. (2024). Manual on information systems (IS) audit 2024. Comptroller and Auditor General of India.

CAG India. (2026). SAI India digital public infrastructure audit guidelines. Comptroller and Auditor General of India, New Delhi, April 2026.

CGAP. (2024). How digital innovation is powering Latin America's financial inclusion. Consultative Group to Assist the Poor.

CGAP. (2025). CGAP Annual Report 2025. Consultative Group to Assist the Poor.

G20 Task Force on DPI. (2023). Report of India's G20 Task Force on digital public infrastructure (v5, November 2023). Ministry of Finance, Government of India.

G20 GPFI. (2023). DPI approach: Towards innovation, resilience, efficiency and inclusive growth for achieving SDGs.

GSMA. (2025). State of the industry report on mobile money 2025. GSMA.

IFAD. (2024). Promoting financial inclusion through digitalisation of remittances (GPFI Report, June 2024).

IMF. (2024). Stacking up the benefits: Lessons from India's digital journey. IMF Working Paper.

INTOSAI WGITA. (2025). 34th annual meeting outcomes: 2026-28 work plan adopted. Hyderabad, September 2025.

MeitY. (2025). Digital personal data protection rules 2025. Ministry of Electronics and Information Technology.

NPCI. (2025). UPI product statistics 2024-25. National Payments Corporation of India.

OECD. (2025). Digital public infrastructure. In Government at a glance 2025. OECD Publishing.

OECD. (2026). Strengthening digital public infrastructure and data governance. In Digital government outlook 2026. OECD Publishing.

South Africa GPFI. (2025). G20 GPFI 2025 plenary outcomes. G20 South Africa Presidency.

UIDAI. (2025). Annual authentication statistics 2024-25. Unique Identification Authority of India.

United Nations. (2024). Universal DPI safeguards framework. UN Digital Economy agenda

World Bank. (2024). ID4D global dataset 2024. Identification for Development Initiative.

World Bank & IDB. (2024). Unlocking the potential of DPI in Latin America and the Caribbean. World Bank Group.

# From India Stack to Citizen Stack: India's DPI Journey and a Blueprint for the World

Karan Vohra &
Keshav Bhardwaj
India





## Abstract

Digital Public Infrastructure (DPI) has emerged as a transformative paradigm in global development discourse, shifting focus from siloed, proprietary technology solutions to shared, interoperable digital systems built on open standards. This article traces India's pioneering DPI journey,from the India Stack, structured around the foundational layers of digital identity (Aadhaar), payments (UPI), and consent-based data exchange, to the globally oriented Citizen Stack anchored in five guiding "DPI Sutras." It examines India's distinctive "middle-path" model, in which publicly governed infrastructure coexists with private-sector innovation, and documents its measurable impact: expanded financial inclusion, plugged welfare leakages through Direct Benefit Transfers, and a globally dominant real-time payments ecosystem. The article makes the case for global replication of this model, arguing that battle-tested, open-source digital rails offer developing nations a sovereign, equitable alternative to corporate monopolies and surveillance architectures, and a powerful accelerator for achieving the Sustainable Development Goals.

## Keywords

Digital Public Infrastructure, India Stack, Citizen Stack, Aadhaar, UPI, Digital Public Goods, DPI Sutras, financial inclusion

## Introduction

The global discourse surrounding digital transformation has undergone a profound structural shift in recent years, pivoting from a focus on siloed, proprietary technological solutions toward the functional concept of Digital Public Infrastructure (DPI). To fully comprehend the impact and

exportability of India's digital trajectory, it is imperative to first establish a contextual understanding of what DPI entails, how it is defined by international institutions, and why it has emerged as a critical driver for sustainable development.

Historically, digital infrastructure was often conflated with physical connectivity, *viz.* broadband networks, mobile towers, and data centres. However, as the digital economy matured, international bodies such as the World Bank, the United Nations Development Programme (UNDP), and the G20 began to redefine DPI as a set of shared digital systems designed to deliver equitable access to public and private services at a societal scale.[1] The first internationally accepted definition was formalised in the G20 New Delhi Leaders' Declaration of September 2023, which described DPI as a set of shared, secure, and interoperable digital systems built on open standards to unlock innovation and solve problems at a population scale.[2]

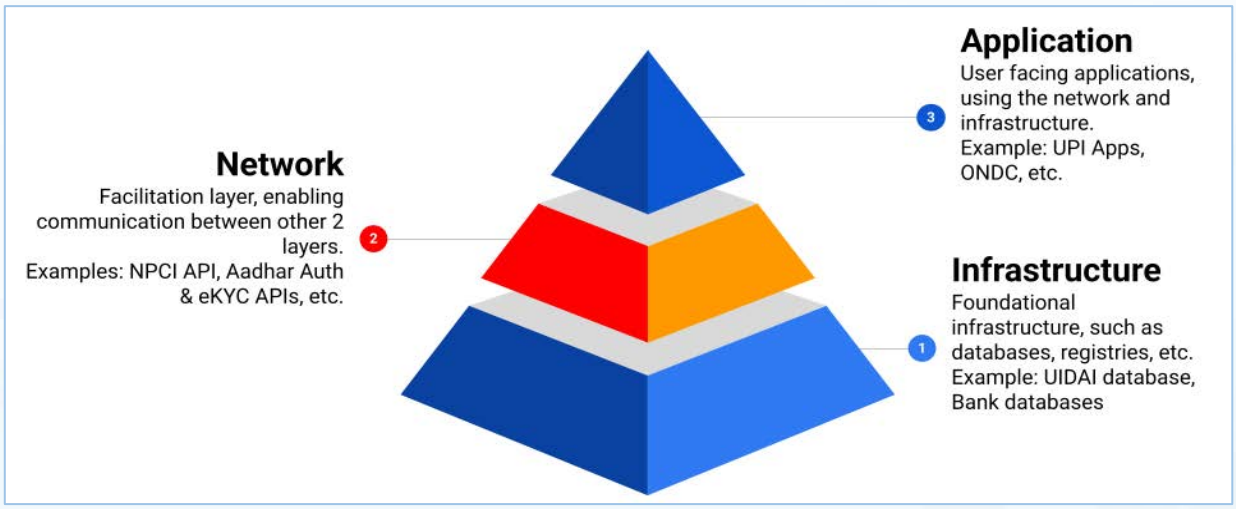



**Fig. 1: 3-layer DPI Framework**

The academic and policy debate surrounding DPI generally oscillates between two frameworks: understanding DPI as a functional category of specific digital systems, and viewing it as a broader conceptual approach to digital transformation. The functional approach identifies three core pillars: digital identity, digital payments, and secure data exchange.[3] Conversely, the "DPI as an approach" framework emphasises the application of foundational, reusable digital building blocks for the public benefit, regardless of whether the government or the private sector operates them, provided they are governed by robust rules that prioritise inclusivity, privacy-by-design, and user-centricity.

The global imperative for deploying DPI is driven by stark developmental deficits. Currently, approximately 2.9 billion people, predominantly in Sub-Saharan Africa and South Asia, lack a formal digital identity, which systematically excludes them from online transactions, formal banking, and targeted government welfare. Furthermore, only 8 per cent of lower-middle-income countries and 16 per cent of upper-middle-income countries possess fast, inclusive payment systems.[4] Traditional approaches to digitising governance have often resulted in

fragmented strategies, high institutional capacity burdens, and vendor lock-in with private technology firms that extract monopolistic profits.[5]

By contrast, the DPI approach advocates for treating digital capabilities such as verifying who someone is, transferring value, and sharing credentials as essential civic utilities, analogous to roads or power grids. By establishing these capabilities as interoperable public protocols, countries can shift competition away from the infrastructure layer and toward the service layer, thereby allowing public agencies and private enterprises to build innovative applications atop a shared digital foundation.

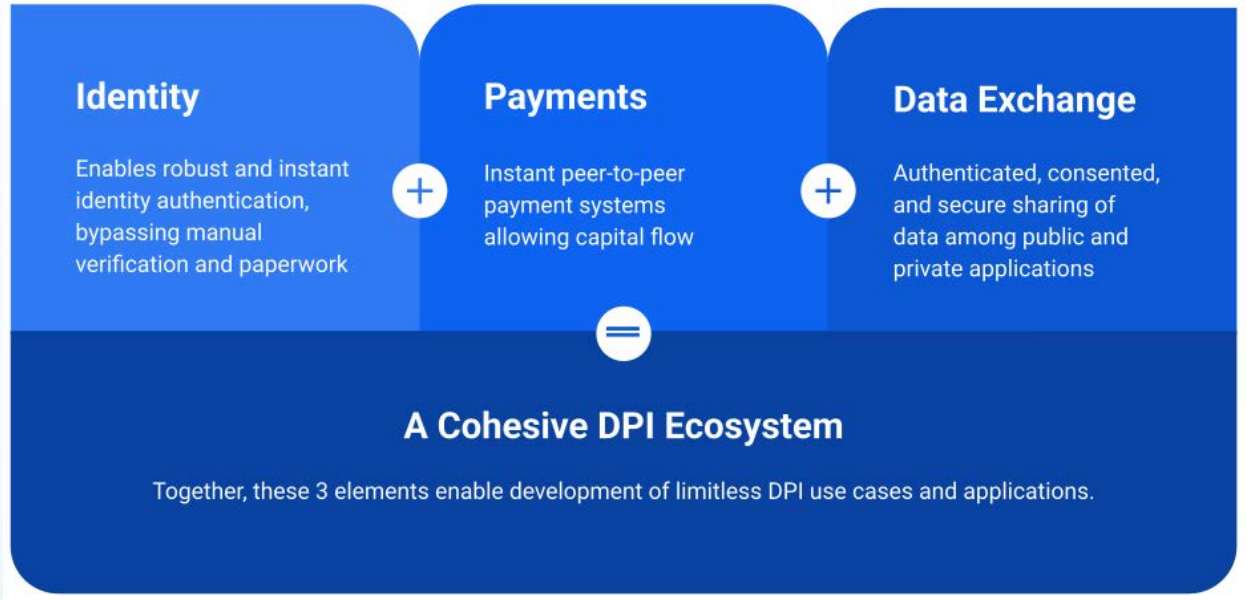



**Fig. 2: DPI Ecosystem**

## India's DPI Stack: *India Stack*

India's decade-long endeavour to construct a nationwide digital public infrastructure, collectively known as the *India Stack*, represents a paradigmatic case of how a state can design and implement digital infrastructure to foster socioeconomic transformation. Evolving from disparate e-government initiatives in the early 2000s, India's DPI was systematically developed into a cohesive, horizontal platform structured around three foundational, interoperable layers. The structural evolution of the India Stack relied heavily on what researchers term "behavioural institutionalism." This concept suggests that the effectiveness of India's digital architecture stems from its ability to combine institutional design with behavioural acumen. By sequentially rolling out identity infrastructure prior to payments, and establishing payments prior to complex data exchange frameworks, the state facilitated an iterative building of public trust and user familiarity.[6]

The architecture of India's DPI deliberately eschews the fully state-run surveillance models seen in some jurisdictions, as well as the heavily corporatised, market-led digital monopolies prevalent in others. Instead, as evaluated in the inaugural *State of DPI in India* report by the

Center for Digital Public Goods (CDPG) at IIM Bangalore, India pioneered a global "middle-path" model.[7] In this framework, the core infrastructure is built as a public layer with strict regulatory guardrails to prevent predatory corporate practices and misuse, while the private domain is encouraged to innovate and drive customer responsiveness on top of these public rails.[8]

India Stack's architecture systematically addresses all three fundamental frictions of a modern economy: the flow of people (identity), the flow of money (payments), and the flow of information (data exchange).

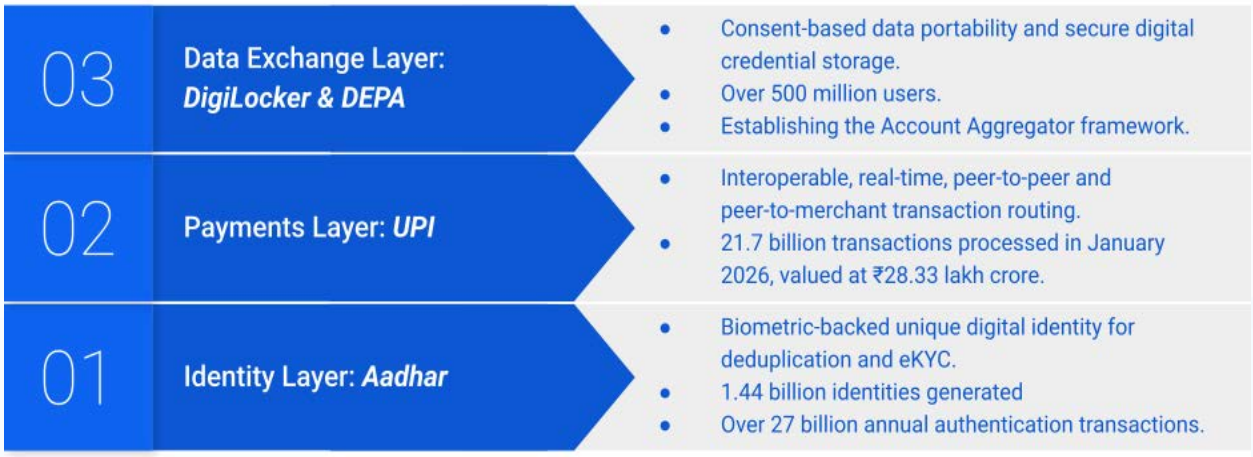



**Fig. 3: India Stack Layers**

## From India Stack to Citizen Stack

As India accelerates the global export of its digital infrastructure, the narrative has evolved from the domestically focused "India Stack" to a globally applicable "Citizen Stack." Unveiled prominently during a United Nations conference in April 2024, the Citizen Stack is envisioned as an open-source playbook for the world, demonstrating how to align digital public infrastructure with inclusive societal goals.[9] The transition to the Citizen Stack represents a philosophical shift from merely exporting technology to sharing a trusted, citizen-centric digital ecosystem that prioritises human rights and digital sovereignty. To define what constitutes a "good DPI" within this global framework, the Citizen Stack is anchored by five guiding principles, known as the "DPI Sutras". These non-negotiable principles ensure that digital infrastructures act as true public goods:

1. **Citizen's Agency and Privacy:** Safeguarding citizen empowerment by upholding a consent-based system for sharing data, free from adverse state or market influences.
2. **Interoperability:** Ensuring open standards to prevent citizens from being locked in by competing digital monopolies.
3. **Techno-Legal Regulation:** Combining public technology architectures with robust legal frameworks to govern ethical tech use and protect societal rights.

4. **Bypassing Private Monopoly (Public Plus Private Innovation):** Fostering a model where core infrastructure remains public, but private innovation flourishes on top, preventing domination by corporate interests.
5. **Safeguarding Against Weaponisation:** Ensuring technology implementations avoid creating hooks for weaponisation by state or corporate actors.

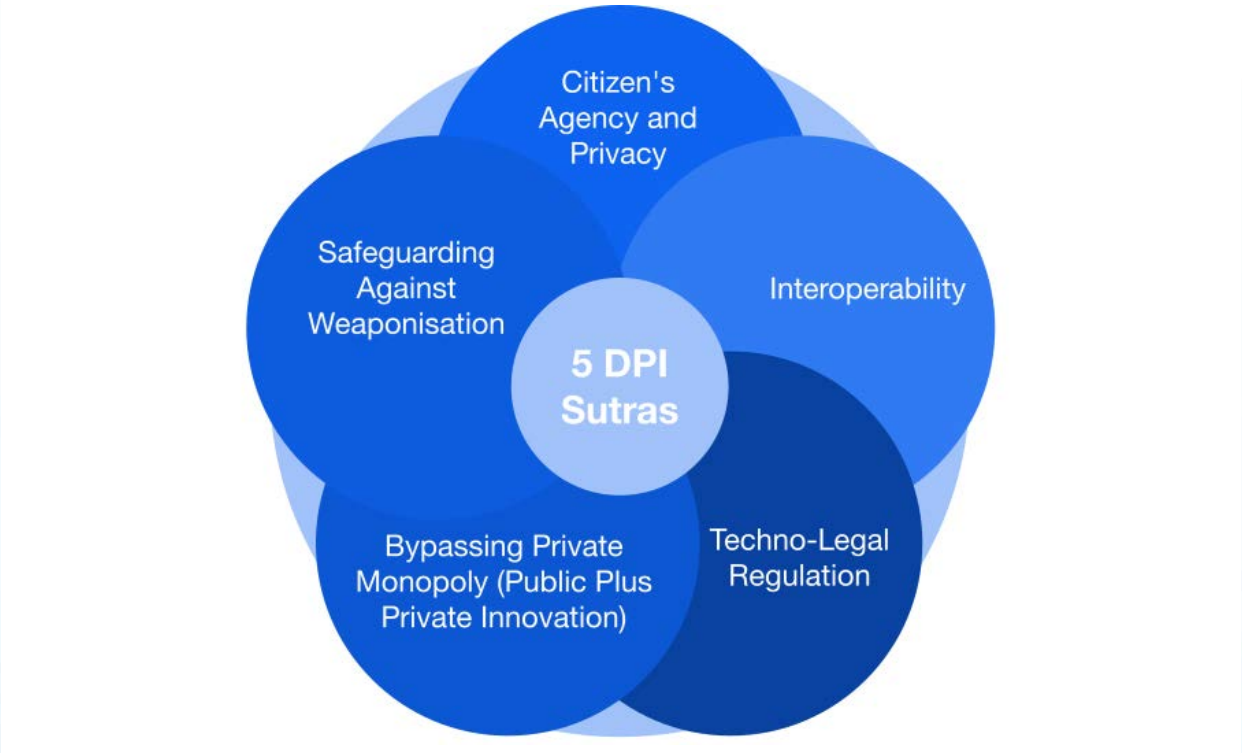



**Fig. 4: DPI Sutras**

By adhering to these sutras, the Citizen Stack ensures that these digital rails empower individuals rather than exploit them, setting a gold standard for global DPI implementation.

## Impact of India's DPI

DPI has facilitated rapid formalisation and operational efficiency. The synthesis of Jan Dhan (zero-balance bank accounts), Aadhaar, and mobile connectivity constitutes the "J-A-M Trinity," providing the necessary endpoints, verification layers, and communication channels for a massive overhaul of the Indian welfare state.

This JAM infrastructure operationalised the Direct Benefit Transfer (DBT) mechanism, creating an unmediated digital pipeline from the central treasury directly to the citizen's bank account. Using the Aadhaar Payment Bridge (APB) and the Public Financial Management System (PFMS), the government dynamically routes funds using the citizen's Aadhaar number as a financial address, bypassing local intermediaries or cash payments. [10]

The scale and fiscal efficiency of this transformation are unprecedented globally. As of early 2026, the DBT framework supports over 316 central government schemes and more than 2,000 sub-national programmes, with cumulative disbursements exceeding ₹49.09 lakh crore.[11]

The integration of digital payments helped boost sales for micro-enterprises and firms operating in the informal sector. Firms that adopted novel DPI-enabled payment technologies observed a 26 per cent improvement in sales relative to their non-adopting peers.[12] Furthermore, private organisations leveraging DPI frameworks reported enhanced operational efficiencies, including an 8 per cent higher conversion rate in SME lending, a 65 per cent reduction in depreciation costs, and a 66 per cent reduction in costs related to fraud-detection for some Non-Banking Financial Companies (NBFCs).[13]

The sheer volume of digital commerce flowing through the Unified Payments Interface underscores this market transformation. In the fiscal year 2025-26, UPI processed 241.6 billion transactions, a nearly 12,000-fold surge in volume over its decade of operation. The annual transaction value exceeded ₹314 lakh crore ($3.29 trillion), meaning that UPI now captures approximately 49 per cent of global real-time payment volume.[14] This high-frequency retail usage demonstrates that DPI has transitioned from a novel technological experiment into the indispensable circulatory system of the Indian economy.

## Case for Global Replication

The rationale for replicating India's DPI globally is deeply rooted in the structural limitations and inequities of the prevailing digital status quo. The dominant models of global digital infrastructure have largely bifurcated into two restrictive paradigms: proprietary platforms operated by profit-driven transnational technology monopolies that aggressively monetise user data, and highly centralised, closed architectures designed for state surveillance. The Indian approach offers a democratic, equitable third alternative. By abstracting essential digital functions *viz.* identity verification, financial routing, and data sharing into open-source public protocols, nations can preserve digital sovereignty, foster intense private sector competition at the service layer, and dramatically accelerate their developmental trajectories.

India's ancient ethos of *Vasudhaiva Kutumbakam,* meaning "the world is one family", finds its most natural digital expression in DPI, as Digital Public Goods (DPGs) evolve into Global Digital Public Goods (GDPGs). Under this vision, India approaches its digital architecture not as a proprietary export to be monetised, but as a GDPG intended for inclusive, equitable development across the Global South and beyond. By offering open-source frameworks, India’s DPI Stack ensures that developing nations can adopt transparent, citizen-centric technologies without falling into the trap of data-centric commercial models or restrictive vendor lock-ins with foreign tech giants. This model prioritises collective global progress, empowering partner nations to build scalable infrastructure while maintaining full sovereign control over their citizens' data.[15]

A crucial argument for global replication is the ability of partner nations to leverage highly mature, battle-tested digital rails. India has spent over a decade refining the India Stack to handle the unprecedented scale of 1.4 billion people, iterating on critical components like biometric deduplication, real-time settlement, and fraud mitigation. By adopting these proven architectures, such as the Modular Open Source Identity Platform (MOSIP) for identity or integrating with UPI frameworks for payments, interested developing nations do not need to reinvent the wheel. Instead, they can bypass decades of expensive trial and error, immediately deploying robust, population-scale infrastructure that has already proven its resilience in complex, low-resource, and highly diverse demographic environments.

The most compelling argument for the global replication of DPI is its unparalleled capacity to act as a catalyst for the United Nations Sustainable Development Goals (SDGs). As empirically demonstrated in India, establishing a foundational digital identity is the crucial first step in securing legal status and human rights for the world's most vulnerable populations. Providing the 2.9 billion undocumented individuals globally with a secure identity via Aadhaar-inspired platforms such as MOSIP is a prerequisite for subsequent access to healthcare, education, and social safety nets.

Moreover, interoperable fast payment systems fundamentally alter the economics of poverty. By reducing the overhead costs associated with domestic and cross-border remittances, DPI ensures that migrant capital flows directly to families rather than being absorbed by intermediary financial institutions. The implementation of secure, consent-based data-sharing frameworks similarly democratises access to credit. In emerging markets and developing economies, micro, small, and medium-sized enterprises (MSMEs) face a staggering financing gap; women-owned MSMEs alone account for 34 per cent of it (equivalent to $1.9 trillion). DPI allows these enterprises to leverage alternative digital footprints, such as real-time payment histories, to secure working capital, thereby driving systemic economic formalisation and productivity.[16]

In particular, India's DPI Stack has been recognised by the United Nations Development Programme (UNDP) as a potent accelerator of the SDGs. In a G20 policy document, the UNDP explicitly mapped India's functional DPI pillars to specific global targets. For instance, to help eradicate poverty (SDG 1), the deployment of Aadhaar established a secure, interoperable digital identity that facilitated contactless direct benefit transfers. By plugging systemic leakages in public welfare and wage payments, this foundational ID system demonstrated up to a 13.4 per cent improvement in household incomes.[17]

## Conclusion

The conceptualisation, evolution, and maturity of India's Digital Public Infrastructure stand as a masterclass in leveraging technology for population-scale socioeconomic inclusion. By treating digital identity, interoperable payments, and consent-driven data exchange as essential public

utilities rather than proprietary commodities, the India Stack has systematically dismantled barriers that previously alienated hundreds of millions from the formal economy. The empirical outcomes are undeniable: a near fifty-year leap in financial inclusion achieved in six years[18], billions of dollars in optimised fiscal expenditure, and the cultivation of a globally dominant real-time retail payment ecosystem.

Through the strategic export of open-source frameworks like MOSIP, and the bilateral internationalisation of UPI, India is providing developing nations with the blueprints to achieve true digital sovereignty. While complex regulatory harmonisation and infrastructure gaps remain formidable challenges, the widespread adoption of the DPI model offers the most viable, equitable pathway to accelerating the Sustainable Development Goals. By embracing these digital public goods, the global community can foster a future where access to the digital economy and services is recognised not as a luxury afforded by private monopolies, but as a fundamental, inclusive civic right.

## References

1. United Nations Development Programme [UNDP]. (2023). Accelerating the SDGs through digital public infrastructure: A Compendium of the Potential of Digital Public Infrastructure. In undp.org. UNDP. Retrieved June 16, 2026, from https://www.undp.org/sites/g/files/zskgke326/files/2023-08/undp-g20-accelerating-the_sdgs-through-digital-public-infrastructure.pdf

2. G20 digital ministers recognize digital public infrastructure as an accelerator of the global goals. (n.d.). UNDP. https://www.undp.org/press-releases/g20-digital-ministers-recognize-digital-public-infrastructure-accelerator-global-goals

3. Global Digital Public Infrastructure Program: From Foundations to Scale. (2026, May 6). https://www.worldbank.org/en/results/2026/05/06/global-digital-public-infrastructure-program

4. Global Digital Public Infrastructure Program: From Foundations to Scale. (2026, May 6). https://www.worldbank.org/en/results/2026/05/06/global-digital-public-infrastructure-program

5. Michael, B. (2026, April 24). What's in a name? Emerging approaches to defining and applying DPI. Center for Financial Inclusion. https://www.centerforfinancialinclusion.org/brief/whats-in-a-name-emerging-approaches-to-defining-and-applying-dpi/

6. Mohanty, P. K. (2026). The Digital Leviathan: How the India Stack Redefined State Capacity in the 21st Century. In Advances in economics, business and management research/Advances in Economics, Business and Management Research (pp. 142–161). https://doi.org/10.2991/978-94-6239-660-9_9

7. Srinivasan, R.; Prabhu, Vikas N.; Sharma, Anuradha; Chakraborty, Nayanika; and Bhoi, Chaitrali, 2025. State of DPI in India, 2025, Center for Digital Public Goods (CDPG), Indian Institute of Management Bangalore (IIMB), October 2025.

8. Srinivasan, R.; Prabhu, Vikas N.; Sharma, Anuradha; Chakraborty, Nayanika; and Bhoi, Chaitrali, 2025. State of DPI in India, 2025, Center for Digital Public Goods (CDPG), Indian Institute of Management Bangalore (IIMB), October 2025.

9. Kamboj, A. R. (2025, March 18). How India's digital public infrastructure can push inclusive global growth. Citizen Stack. https://www.citizenstack.world/post/how-india-s-digital-public-infrastructure-can-push-inclusive-global-growth

10. Bhattacharya, S. R. S. (n.d.). Intent to Implementation: Summary of Lessons from Tracking India's Social Protection Response to COVID-19 (English). World Bank. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/404061625000764344

11. India's DBT: Boosting Welfare Efficiency. (n.d.). https://www.pib.gov.in/PressReleasePage.aspx?PRID=2123192

12. Khera, P. (2023). Digital financial services and inclusion. In A. Schipke, J. Turunen, N. Choueiri, & A. M. Gulde (Eds.), India's financial system: Building the foundation for strong and sustainable growth (Chap. 7). International Monetary Fund. https://doi.org/10.5089/9798400223525.071

13. G20 document prepared by World Bank lauds India's progress. (n.d.). https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=1955516

14. UPI completes 10 glorious years, Emerges as World's Largest Real-Time Payments Platform, Anchoring India's Digital Economy. (n.d.). https://www.pib.gov.in/PressReleasePage.aspx?PRID=2257087

15. Primus Partners, & iSPIRT. (2024). Beyond boundaries: India's digital public infrastructure (DPI) model for global progress. https://primuspartners.in/docs/documents/Beyond%20Boundaries%20-%20India%E2%80%99s%20Digital%20Public%20Infrastructure%20(DPI)%20%20Model%20for%20Global%20Progress.pdf

16. Ardic, O., Galicia Rabadan, G., Marin, G., Natarajan, H., Piveteau, T., Ramteke, N., & Sarkar, A. (2023). G20 policy recommendations for advancing financial inclusion and productivity gains through digital public infrastructure. Global Partnership for Financial Inclusion (GPFI) & World Bank. https://openknowledge.worldbank.org/server/api/core/bitstreams/c5f1fc39-7a91-41e6-9965-6355465b5f72/content

17. United Nations Development Programme [UNDP]. (2023). Accelerating the SDGs through digital public infrastructure: A Compendium of the Potential of Digital Public Infrastructure. In undp.org. UNDP. Retrieved June 16, 2026, from https://www.undp.org/sites/g/files/zskgke326/files/2023-08/undp-g20-accelerating-the_sdgs-through-digital-public-infrastructure.pdf

18. Ardic, O., Galicia Rabadan, G., Marin, G., Natarajan, H., Piveteau, T., Ramteke, N., & Sarkar, A. (2023). G20 policy recommendations for advancing financial inclusion and productivity gains through digital public infrastructure. Global Partnership for Financial Inclusion (GPFI) & World Bank. https://openknowledge.worldbank.org/server/api/core/bitstreams/c5f1fc39-7a91-41e6-9965-6355465b5f72/content



Section II

# THE LAYERS BENEATH: CONNECTIVITY, CLOUD AND LOCATION

# Mapping Municipal Equity: Leveraging Spatial DPI for Inclusive Solid Waste and Utility Management in Smart Cities


## Dr. Nanda Dulal Das

O/o the Comptroller & Auditor General of India





## Abstract

Digital Public Infrastructure (DPI) has emerged as a cornerstone of inclusive development, offering scalable, open-source building blocks that enable societal-scale service delivery. While India's foundational DPI layer has successfully democratised identity and financial payments, its application within municipal urban governance remains highly fragmented. Rapid, market-driven expansion in metropolitan fringes constantly converts peripheral agricultural lands into complex, unorganised peri-urban environments, outpacing formal public utility networks and leaving vulnerable demographics excluded.

This article outlines a unified Geo-DPI framework—integrating open-source satellite remote sensing (RS), Geographic Information Systems (GIS), and public data registries—as a primary mechanism to ensure inclusive governance in smart cities. Drawing comparative insights from progressive municipal utility pricing models implemented in large cities in the USA, including Boston, Seattle, Dallas, and San Francisco, this article shows how unit-based cost-recovery models can be structurally reconfigured for the developing economy context. By combining high-resolution multi-spectral imagery with an automated, census-derived Socioeconomic Vulnerability Index (SVI), the paper introduces a Geospatial Pay-As-You-Throw (PAYT) tariff algorithm.

This model envisages fiscal discipline on commercial and high-income clusters while preserving progressive, targeted subsidies for vulnerable urban populations. Finally, the article demonstrates how the Supreme Audit Institution (SAI) can utilise continuous, independent spatial verification to audit database integrity, combat ecological leakages, and enforce public accountability, translating technical spatial infrastructure into a direct instrument of social and democratic justice.

## Keywords

Digital Public Infrastructure (DPI), Remote Sensing & GIS, Pay-As-You-Throw (PAYT), Urban Equity, Information Systems Audit, Inclusive Governance.

## 1. Introduction

Digital Public Infrastructure (DPI) officially entered the global policy lexicon as a powerful mechanism to accelerate the United Nations Sustainable Development Goals (SDGs), focusing on open, interoperable technology building blocks governed for the common good (Mazzucato, M., Eaves, D., & Vasconcellos, B. 2026). True DPI is distinguished from isolated IT systems by three vital characteristics: interoperability through open standards, execution via reusable modular building blocks, and the creation of exponential societal value through a transparent governance framework (Kapoor, A., & Watson, E. 2023; Mazzucato, M., Eaves, D., & Vasconcellos, B. 2026).

Modern urbanization in developing economies is defined by an intense demographic and physical reconfiguration. In India, urban centres occupy a mere 3% of the nation's land mass but generate over 60% of its Gross Domestic Product (GDP) (NITI Aayog, 2022). This economic density triggers rapid spatial transformations, expanding urban sprawls into peripheral zones and creating a fragmented peri-urban landscape (Bhatnagar, 2026; Kaushik & Kakoty, 2025). Research indicates that roughly 90% of municipal solid waste (MSW) is mismanaged through open dumping and unengineered landfilling. This widespread practice severely threatens ecological balance and public health while actively introducing toxins into the food chain. Consequently, Indian Urban Local Bodies (ULBs) face monumental hurdles in managing these massive waste volumes due to systemic infrastructure deficits compounded by surging population densities (Meena et al., 2023). Traditional municipal services are structurally unequipped to handle this rapid growth; historical evaluations reveal that nearly 30% to 40% of solid municipal waste is routinely left on city streets uncollected daily, with peripheral or marginalized communities bearing the brunt of this civic neglect (Mathur et al., 2007).

The New Urban Agenda mandates that human settlements must be redesigned, financed, and governed to ensure resilience and systemic inclusion, especially for the urban poor (United Nations, 2017). To achieve this goal, cities must move past reactive, siloed IT platforms and embrace an interoperable Geo-DPI infrastructure. By embedding satellite remote sensing (RS) data, digital cadastral maps, and spatial analytics directly into public utility systems, governments can use spatial data as a universally shared resource to optimize public services and guarantee urban equity.

This article seeks to establish a clear technical and methodological blueprint for a Geo-DPI framework designed to manage municipal solid waste (MSW) lifecycles and dynamically recalculate progressive utility tariffs, ensuring no urban community remains invisible.

## 2. Designing a Spatial DPI for Smart MSW Lifecycles

The uncontrolled expansion of urban borders into adjacent agricultural territories generates severe socio-environmental consequences, resulting in intense landscape degradation and structural gaps in public utility networks. In these fringe environments, municipal solid waste management systems frequently suffer from data lags and lack of institutional coverage. Unsanctioned open dumping and open waste burning proliferate, creating long-term environmental risks including systemic biodiversity loss, groundwater contamination, and air pollution. To establish a responsive, real-time civic response, municipal systems require a continuous spatial monitoring engine built on open-tier geospatial data registries.

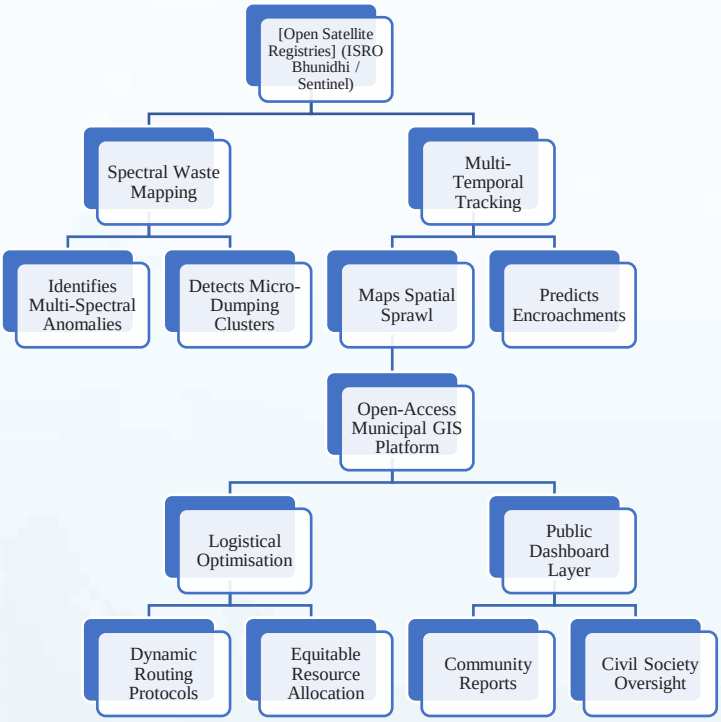



**Figure 1: Spatial DPI Architecture for Smart MSW Lifecycles**

As illustrated in Figure 1, the core architecture of this spatial DPI model uses open-access, high-resolution satellite remote sensing registries—such as India's ISRO Bhunidhi or Europe's Sentinel (Copernicus) platforms—as a baseline public data source. Automated image processing networks continuously can run change-detection routines across municipal boundaries.

By analysing specific multi-spectral anomalies and pixel variations, the system maps the distinct signatures of plastic debris, organic decay, and industrial waste piles, pinpointing unauthorised micro-dumping spots long before they scale into unmanageable regional landfills. Simultaneously, multi-temporal spatial analysis monitors the directional expansion of peri-urban growth, allowing municipal administrators to predict future infrastructure requirements and allocate collection resources proactively.

This rich spatial database translates directly into an open-access Geographic Information System (GIS) tailored for equitable municipal logistics. Traditional municipal waste dispatch structures usually rely on static, historical route planning that naturally prioritises high-revenue commercial corridors while overlooking informal or peripheral settlements. Real-time spatial and route planning can improve this scenario dramatically (Del Carmen-Niño et.al. 2023).

By integrating automated, real-time spatial waste data with open GIS vehicle routing algorithms, cities can dynamically adjust fleet paths based on actual waste accumulation density rather than property status (Prata et al., 2025). This ensures that municipal sanitation trucks service low-income fringe neighbourhoods with the same efficiency and frequency as affluent commercial zones, eliminating structural municipal neglect and protecting the health of vulnerable citizens.

## 3. Reimagining Utility Rate Frameworks: Global Models to Indian Realities

To achieve sustainable urban cost recovery while protecting the poor, cities must link individual usage behaviour directly with fair financial incentives (Vesmaș et al., 2026). The US Environmental Protection Agency (EPA) highlights Unit-Based Pricing, commonly known as Pay-As-You-Throw (PAYT), as the most effective municipal strategy to minimise household trash output, boost recycling compliance, and limit local greenhouse gas emissions (Barry, 2017). In pioneering cities like Seattle and San Francisco, PAYT schemes charge residents a variable, per-unit fee based on the exact volume or weight of the waste they discard. Long-term economic data from these implementations confirm a clear, statistically significant correlation between variable PAYT structures and systemic household waste reduction (Barry, 2017).

However, blindly importing a Western PAYT model into a developing country's urban fabric will inevitably worsen social inequities. In cities with wide income disparities, flat volumetric pricing acts as a regressive tax, placing a disproportionate financial burden on low-income families who spend a larger percentage of their income on basic survival utilities. To prevent this, the municipal Geo-DPI engine must fuse consumption proxies with an automated, spatialized Socioeconomic Vulnerability Index (SVI).

The technical implementation of this model requires the seamless integration of four distinct spatial and database infrastructure layers:

a. **The Spatial Cadastral Base:** Digitised property parcels linked directly to GIS attribute records, establishing a unique spatial index for every residential and commercial structure.

b. **The Consumption Proxy Grid:** In areas lacking expensive smart-metering hardware, the platform uses multi-spectral thermal bands to estimate building utilisation scales and population density models to generate baseline volumetric consumption metrics.

c. **The Socioeconomic Vulnerability Layer:** A normalised index derived from localised census data, average regional land values, and public distribution data, standardising socio-spatial privilege on a 0-to-1 scale.

d. **The Algorithmic Engine:** The platform applies advanced statistical regressions to balance municipal financial sustainability with citizen affordability, ensuring that local variables—such as proximity to collection networks or regional income medians—are factored in to prevent inequitable pricing (Prata et al., 2025).

To dynamically calculate an equitable, progressive municipal utility charge (F_i) for any target spatial parcel (i), the engine uses the following mathematical formula:

$$F_i = (V_i \times R_b \times [C_i / R_a]) \times (1 - SVI_i)$$

Where:

i. **F_i** = The dynamic monthly municipal utility or waste fee calculated for target spatial parcel *i*

ii. **V_i** = The estimated or physically verified volumetric waste output proxy of the parcel

iii. **R_b** = The standard baseline municipal cost-recovery rate per unit of utility service

iv. **C_i / R_a** = The localised ratio of Commercial-to-Residential land-use intensity, designed to automatically scale tariff rates for high-profit commercial property footprints.

v. **SVI_i** = The normalised Socioeconomic Vulnerability Index score of the target cluster grid, scaled precisely between 0 and 1.

By embedding the $(1 - SVI_i)$ modifier directly into the core pricing equation, the Geo-DPI platform builds targeted financial relief into the code. High-intensity commercial entities and affluent estates pay an escalated cost-recovery rate, while the system automatically applies progressive financial subsidies to marginalized urban grids, preserving their access to vital public infrastructure.

## 4. Prototype Simulation: Ward 45 (Peri-Urban Fringe, Sector B)

To visualise how the Geo-DPI engine processes spatial data into equitable utility tariffs, we analyse a real-world prototype scenario tracking three distinct urban properties within a dynamic peri-urban ward.

### 4.1 The Inputs: Datasets & Layer Overlay Matrix

The Geo-DPI engine synthesises data from the core infrastructure layers to establish the baseline parameters for each property (Table 1):

**Table 1: Establishment of Baseline Parameters for different types of Properties**

| Baseline Infrastructure Data Layers | Property A: "Greenfield Heights" (Affluent Residential Estate) | Property B: "Kalyan Nagar Cluster" (Low-Income Settlement) | Property C: "Mega-Mart Logistics" (High-Intensity Commercial Hub) |
|---|---|---|---|
| **Layer 1: Spatial Cadastral Base** | **ID:** parcel_45_001<br>**Footprint:** 4,500 sq. meters<br>**Zoning:** Residential | **ID:** parcel_45_042<br>**Footprint:** 65 sq. meters<br>**Zoning:** Residential | **ID:** parcel_45_108<br>**Footprint:** 12,000 sq. meters<br>**Zoning:** Commercial |
| **Layer 2: Consumption Proxy Grid** (Spectral Volume) | **High Volumetric Output:** Large physical footprint and high structural density map a baseline proxy of 4.5 units of weekly waste generation. | **Low Volumetric Output:** Minimal physical footprint maps a baseline proxy of 0.8 units of weekly waste generation. | **Maximal Volumetric Output:** High-velocity commercial signatures map a baseline proxy of 12.5 units of weekly waste generation. |
| **Layer 3: Socioeconomic Vulnerability Layer** (Normalised) | **Low Vulnerability:** Located in a high-land-value grid with 100% formal civic tenure.<br>**Score = 0.05** | **High Vulnerability:** Located in an unorganized, low-income peripheral grid.<br>**Score = 0.75** | **Zero Vulnerability Modifier:** Corporate commercial entity.<br>**Score = 0.00** |

**Standard Base Cost-Recovery Rate:** ₹100 per unit of municipal service.

**Commercial Land-Use Intensity Ratio:** Set to 1.00 for standard residential parcels, and automatically escalates to 2.50 for heavy commercial zones.

## 4.2 The Algorithmic Engine Pricing Outputs

By running the properties through the linear text-compatible formula/equation, the engine yields the following distinct municipal fiscal assessments (Table 2):

**Table 2: Distinct Municipal Waste Fee Assessments**

| Property | Property Type | Waste Fee/sq. meters |
|---|---|---|
| **Property A** | Affluent Residential | ₹427.50 |
| **Property B** | Low-Income Subsidized | ₹20.00 *(Automatically protected via spatial equity modifiers)* |
| **Property C** | Commercial Cost Recovery | ₹3,125.00 *(Escalated commercial cost recovery applied)* |

# 5. The Spatial Auditor's Perspective: Ensuring Fiscal Accountability and Social Inclusion

When a municipality transitions its public utility delivery and fee calculations to automated digital infrastructure, the Supreme Audit Institution (SAI) must shift its oversight strategies accordingly. Information Systems (IS) and environmental auditors can no longer rely on simple paper trails; they must audit the technical data pipelines, algorithmic parameters, and systemic outputs of the Geo-DPI platform to prevent corruption and ensure equity.

Spatial auditors can implement a rigorous validation strategy divided into three core stages:

a. **Data Pipeline Integrity Audits:** Auditors can examine database schemas and interface connections to ensure that municipal tax profiles match real-world property dimensions, preventing elite tax evasion and database manipulation.

b. **Independent Change-Detection Audits:** Using independent, third-party satellite data sourced directly from scientific space registries, auditors can perform automated spatial comparison routines. By overlaying independent satellite-derived maps onto the municipal service log, auditors can easily catch under-reported peripheral dump sites or detect if low-income clusters are being left off sanitation routes.

c. **Algorithmic Fairness Testing:** Auditors can run spatial regression models to verify the calculations of the pricing engine. This testing ensures that the Socioeconomic Vulnerability Index modifiers are executing correctly across all municipal sectors and that public subsidies are reaching intended beneficiaries without leakage.

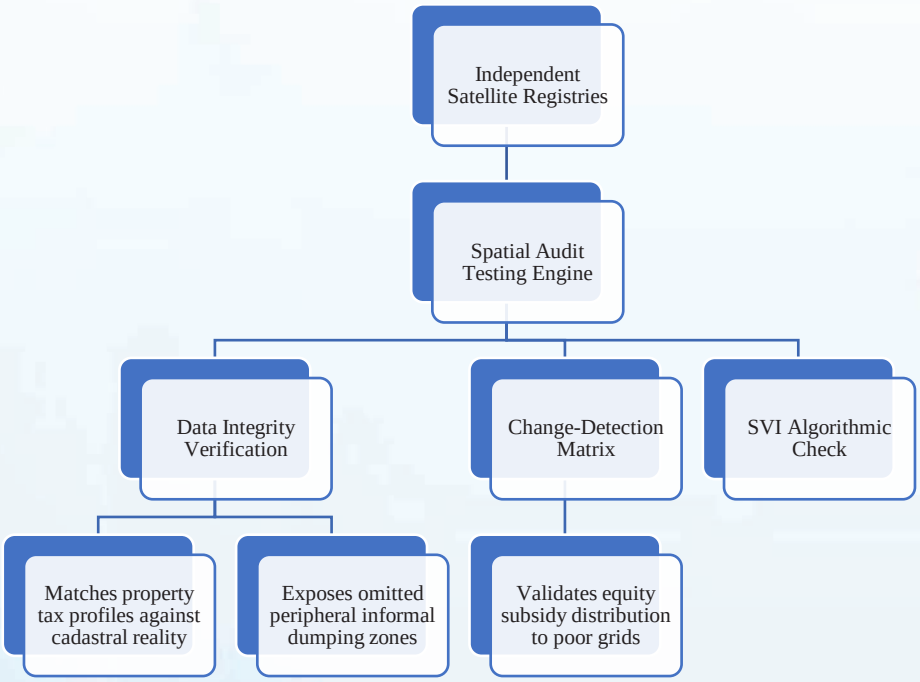



**Figure 2: Spatial Audit Verification Framework**

As shown in Figure 2, this independent verification loop provides an objective check on municipal performance. Furthermore, by publishing these audited geospatial maps onto open-access public audit dashboards, the SAI can turn complex data into an accessible tool for civic oversight. When citizens, local community boards, and international development organisations can easily see verified maps of fund utilisation, service coverage, and subsidy allocation, the audit function moves beyond simple bureaucratic box-checking to drive true community empowerment and democratic transparency.

## 6. Prototype Simulation Matrix for Figure 2: Operationalising the Spatial Audit

This simulation shows how the spatial audit engine cross-references municipal records against independent satellite data within Ward 45 (Sector B) to flag anomalies, calculate fiscal leakages, and identify systemic exclusions (Table 3).

**Table 3: Spatial Audit Testing Engine Ledger (Ward 45 Core)**

| Audit Verification Stage | Target Dataset & Source Layer | Systemic Flag / Anomaly Trigger | Computed Audit Resolution & Impact |
|---|---|---|---|
| **Stage 1: Data Integrity Verification** (Elite Tax Evasion Check) | **Municipal Ledger:** Property Tax Database<br>**Spatial Baseline:** Digitised Cadastral Plot Boundaries | **Discrepancy Detected:** Parcel **parcel_45_001**("Greenfield Heights") was registered as a 500 sq. meter standard plot. The independent cadastral GIS geometry calculates the true built-up layout at 4,500 sq. meters. | **Action:** Auditor flags the entry for under-reporting.<br>**Fiscal Recovery:** Recomputed baseline tariff scales from ₹47.50 to ₹427.50, preventing local tax leakage. |
| **Stage 2: Change-Detection Matrix** (Omitted Service Tracking) | **Municipal Log:** 100% Waste Collection Clearance Loop<br>**Independent Evidence:** ISRO Bhuvan Multi-Spectral Bands | **Discrepancy Detected:** Near **parcel_45_042** ("Kalyan Nagar Cluster"), satellite imagery flags a highly distinct multi-spectral signature indicating high-density plastic and organic accumulation. | **Action:** Auditor issues an immediate logistical exception log: *"Systemic fleet omission detected at Grid 45-B."*<br>**Inclusion Impact:** Forces immediate deployment of physical sanitation trucks to a marginalised area. |
| **Stage 3: SVI Algorithmic Check** (Subsidy Flow Validation) | **Engine Code:** Array Logic<br>**Socio-economic Layer:** Localised Census & Land Value Grids | **Discrepancy Detected:** The system successfully mapped a 75% relief modifier to low-income grids without letting the subsidy bleed into adjacent commercial zones. | **Action:** Auditor validates algorithmic fairness across the sector.<br>**Inclusion Impact:** Confirms targeted public funds are reaching intended beneficiaries with zero leakage. |

## 7. Discussion and Conclusion

Implementing an open, interoperable Geo-DPI framework offers a powerful solution to the structural inequities of modern smart cities. By anchoring municipal solid waste tracking and utility pricing models in transparent geospatial infrastructure, cities can replace fragmented, exclusive administration with a system focused on data-driven social justice. This model aims that municipal cost recovery and fiscal sustainability do not require sacrificing equity for the poor; by utilising spatial metrics and built-in vulnerability modifiers, public utilities can preserve financial viability while actively protecting vulnerable communities.

To scale this spatial infrastructure successfully across expanding urban environments, a coordinated policy roadmap needs to be prioritised:

a. **Dismantle Data Monopolies:** Public geospatial records, space registry data, and land parcels must be liberated from isolated departmental silos and integrated into an open, interoperable national DPI ecosystem accessible to public managers, auditors, and civil society.

b. **Build Technical Public Capacity:** Institutional training systems must modernise their curricula, training public service leaders and oversight officers in technical disciplines like Python, SQL, GIS applications, and advanced statistics to ensure effective management and auditing of automated platforms.

c. **Mandate Spatial Audit Frameworks:** Independent geospatial verification must be institutionalised as a core requirement for evaluating large-scale urban development programmes, ensuring public fund allocation matches real-world execution.

Ultimately, the future of inclusive governance depends on making the invisible visible. By utilizing an open spatial digital public infrastructure, Supreme Audit Institutions and progressive urban managers can ensure that the smart cities of tomorrow are not merely technologically advanced, but are fundamentally equitable, fair, and accountable to every citizen.

### References

1. Barry, T. W., IV. (2017). When trash costs money: Analyzing the impact of pay-as-you-throw programs in Massachusetts. *Journal of Environmental and Resource Economics at Colby*, *4*(1), Article 3. https://digitalcommons.colby.edu/jerec/vol4/iss1/3/
2. Bhatnagar, S. (2026, June 12). In Varanasi, fringe expansion vs. core heritage. *Governance Now*. https://www.governancenow.com/views/columns/in-varanasi-fringe-expansion-vs-core-heritage
3. Del Carmen-Niño, V., Herrera-Navarrete, R., Juárez-López, A. L., Sampedro-Rosas, M. L., & Reyes-Umaña, M. (2023). Municipal Solid Waste Collection: Challenges, Strategies and Perspectives in

the Optimization of a Municipal Route in a Southern Mexican Town. Sustainability, 15(2), 1083. https://doi.org/10.3390/su15021083

4. Kapoor, A., & Watson, E. (2023). Defining the Digital Public Infrastructure Approach (T20 Policy Brief Task Force 2). Think20 (T20) India 2023. https://t20ind.org/research/defining-the-digital-public-infrastructure-approach/
5. Kaushik, P., & Kakoty, S. (2025). Is the blue-green infrastructure (BGI) key to sustainable development of South Asian cities? In *Sustainability in South Asian cities*. Springer Nature Singapore. https://www.springerprofessional.de/en/is-the-blue-green-infrastructure-bgi-key-to-sustainable-developm/50706804
6. Mathur, M. P., Chandra, R., Singh, S., & Chattopadhyay, B. (2007). *Norms and standards of municipal basic services in India* (Working Paper No. 07-02). National Institute of Urban Affairs. https://prod-qt-images.s3.amazonaws.com/indiawaterportal/import/sites/default/files/iwp2/Norms_standards_municipal_basic_services_in_India_NIUA.pdf
7. Mazzucato, M., Eaves, D., & Vasconcellos, B. (2026). Digital public infrastructure and the economics of public value: what is 'public' about DPI? *Journal of Economic Policy Reform*, *29*(2), 113–141. https://doi.org/10.1080/17487870.2026.2662285
8. Meena, M. D., Dotaniya, M. L., Meena, B. L., Rai, P. K., Antil, R. S., Meena, H. S., Meena, L. K., Dotaniya, C. K., Meena, V. S., Ghosh, A., Meena, K. N., Singh, A. K., Meena, V. D., Moharana, P. C., Meena, S. K., Srinivasarao, C., Meena, A. L., Chatterjee, S., Meena, D. K., Prajapat, M., & Meena, R. B. (2023). Municipal solid waste: Opportunities, challenges and management policies in India: A review. *Waste Management Bulletin*, *1*(1), 4–18. https://doi.org/10.1016/j.wmb.2023.04.001
9. NITI Aayog, & Asian Development Bank. (2022, May). *Cities as engines of growth: TA-9508: Strengthening the states for broad based urban development* (Executive summary). https://www.niti.gov.in/sites/default/files/2022-05/Mod_CEOG_Executive_Summary_18052022.pdf
10. Prata, J., Simões, C. L., & Simoes, R. (2025). Improvements to Municipal Solid Waste Collection Systems Using Real-Time Monitoring. Sustainability, 17(4), 1405. https://doi.org/10.3390/su17041405
11. United Nations Human Settlements Programme. (2017). New Urban Agenda. UN-Habitat. unhabitat.org https://www.urbanagendaplatform.org/nua
12. Vesmaș, D.-M., Dragomir, A. N., Bayraktar, D., & Morari, A. (2026). Integrating PAYT and Emerging Technologies for Smart Waste Management: Towards a Circular Economy Framework. Sustainability, 18(7), 3510. https://doi.org/10.3390/su18073510

# Auditing the Connectivity Layer of Digital Public Infrastructure: Lessons from BPK's Performance Audit of the Indonesian Telecommunications Infrastructure Regulatory Agency


Benidiktus Bambang Triasmoro,
Dwi Jatmika Bima Mahatmantara,








Arief Ridhatama,
Achmad Faishal &
Amri Lewa
Audit Board of the
Republic of Indonesia



## Abstract

Digital Public Infrastructure (DPI)—foundational digital building blocks such as digital identity, payment systems, and data exchange registries—relies heavily on robust connectivity to generate inclusive public value, especially for remote and underserved areas. This article examines lessons from the performance audit experience of the Audit Board of the Republic of Indonesia (BPK) regarding telecommunications infrastructure managed by the Telecommunications and Information Accessibility Agency under Indonesia's Ministry of Communication and Digital Affairs (BAKTI Komdigi). By focusing on backbone, middle-mile, and last-mile infrastructure—such as the Palapa Ring, SATRIA-1, and 4G BTS programs—this article frames telecommunications connectivity not as the entirety of DPI, but as its critical enabling layer.

Using a combined performance and information systems audit lens, the analysis identifies six key audit risk areas: targeting and needs assessment, capacity planning and utilization, service quality

and reliability, contract governance and fiscal accountability, monitoring and evaluation, and sustainability and resilience. The article proposes the Connectivity-Inclusion Governance Audit Framework (CIGAF) to structure the assessment of these risks and to help auditors link technical infrastructure issues with public value and inclusion outcomes. This practical framework is designed to help Supreme Audit Institutions (SAIs) assess whether telecommunications investments effectively support inclusive governance. Contributing to the INTOSAI Working Group on IT Audit (WGITA) agenda, this article translates country-level audit experience into transferable audit considerations for auditing large-scale digital infrastructure.

## Keywords

Digital Public Infrastructure, connectivity layer, inclusive governance, performance audit, information systems audit, Supreme Audit Institutions

## 1. Introduction

Digital Public Infrastructure (DPI) has become one of the most important concepts in contemporary public sector digital transformation. The World Bank Group describes DPI as "foundational digital building blocks for the public benefit," while the OECD views it as "secure and interoperable shared digital systems that can support inclusive access to public and private services across society" (Clark et al., 2025; OECD, 2024). DPI is often associated with digital identity, digital payments, data exchange systems, base registries, and reusable digital platforms designed to enable service delivery across multiple sectors (Fetter et al., 2025; United Nations, 2024a). DPI is expected to assist governments in accelerating public service delivery, reducing administrative burdens, improving the targeting of public programs, enhancing transparency, and fostering public trust. The United Nations Global Digital Compact acknowledges digital public infrastructure and digital public goods as vital enablers of inclusive digital transformation and innovation (United Nations, 2024a). The UN E-Government Survey 2024 also points out that digital government should be a driver for sustainable development, inclusion, and effective public institutions (United Nations, 2024b). These developments indicate that DPI is not just a technological agenda but a governance agenda.

However, DPI does not function independently. Its effectiveness depends on a broader digital ecosystem of legal frameworks, institutional coordination, cybersecurity, data governance, digital literacy, affordability, accessibility, and connectivity (United Nations Development Programme, 2023; World Bank Group, 2025). Connectivity serves as the critical enabling condition for all of these factors. Without reliable and meaningful internet access, citizens and public institutions cannot fully reap the benefits of digital identity systems, online public services, telemedicine, or social protection networks (Clark et al., 2025; International Telecommunication Union, n.d.). This is particularly true for archipelagic nations like Indonesia, which faces complex geographical hurdles in ensuring equitable digital connectivity across thousands of islands. Because market-driven telecommunications deployments typically target commercially viable

areas with high population densities, remote, frontier, and disadvantaged regions often require state intervention to bridge the digital divide. Within this context, the Indonesian Telecommunications Infrastructure Regulatory Agency (BAKTI Komdigi) plays a strategic role in advancing equitable telecommunications access by managing the financing of Universal Service Obligations (USO) and supporting ICT infrastructure deployment[1].

BAKTI Komdigi's initiatives span three infrastructure layers: the Palapa Ring (backbone fiber-optic connectivity), SATRIA-1 (satellite-based middle-mile capacity), and 4G BTS programs alongside public internet access facilities (last-mile interventions) (BAKTI, 2023, 2024).

Indonesia's national digital transformation policy further reinforces this structure by categorizing network and infrastructure as a foundational pillar, emphasizing that telecommunications must be assessed as a critical precondition for digital adoption and inclusive governance (Kementerian Komunikasi dan Digital, 2024).

Consequently, this article conceptualizes these telecommunications programs not as the entirety of DPI, but as its connectivity layer. While DPI traditionally refers to shared digital systems like digital identity and data exchange (Clark et al., 2025; OECD, 2024), those systems cannot reach end-users inclusively without underlying connectivity. For Supreme Audit Institutions (SAIs), including BPK, this distinction introduces a nuanced audit challenge. Traditional infrastructure audits often focus on physical completion, budget absorption, and procurement compliance. While these aspects remain essential, they are insufficient for evaluating digital infrastructure as an enabler of inclusive governance. Modern public sector auditing must also ask whether the infrastructure is accurately targeted, if capacity aligns with actual needs, and whether the services yield meaningful, sustainable public benefits. This broader perspective is deeply rooted in the principles of performance auditing (ISSAI 300 and ISSAI 3000) and information systems auditing (GUID 5100) (INTOSAI, 2019e, 2019f, 2019c). BPK's audit practices are governed by the State Financial Audit Standards (SPKN), which adapt the ISSAIs that form a part of the INTOSAI Framework of Professional Pronouncements (IFPP), ensuring alignment with these international standards[2].

The main contribution of this article is the reframing of telecommunications infrastructure audits as an audit of the connectivity layer of DPI. By drawing on BPK's performance audit experience, the article links digital public infrastructure, public sector performance audits, and inclusive governance outcomes. Ultimately, it proposes the Connectivity-Inclusion Governance Audit Framework (CIGAF) as a practical tool to help other SAIs structure audits that evaluate economy, efficiency, effectiveness, and digital inclusion.

---

1 BAKTI Komdigi stands for *Badan Aksesibilitas Telekomunikasi dan Informasi Kementerian Komunikasi dan Digital* (The Telecommunications and Information Accessibility Agency under Indonesia's Ministry of Communication and Digital Affairs). KPU/USO stands for *Kewajiban Pelayanan Universal* (Universal Service Obligation).

2 BPK's audit work is governed by the State Financial Audit Standards (*Standar Pemeriksaan Keuangan Negara* or SPKN). SPKN adapts the ISSAI which is part of INTOSAI Framework of Professional Pronouncements (IFPP), ensuring BPK's audit mandates are aligned with international best practices.

# 2. Digital Public Infrastructure and the Connectivity Layer

## 2.1 Digital Public Infrastructure and Inclusive Governance

Inclusive governance is a fundamental promise of DPI, aiming to empower governments to serve vulnerable and marginalized populations equitably. However, the Universal DPI Safeguards Framework warns that poorly governed DPI can inadvertently heighten barriers for those lacking internet access, devices, or digital literacy (United Nations, 2024c, 2024d). Therefore, evaluating DPI requires looking beyond the mere existence of shared technology platforms to assess true accessibility and usability, which fundamentally relies on a robust connectivity layer.

## 2.2 Connectivity as a DPI-Enabling Layer

The connectivity layer encompasses the networks, transmission capacity, satellite links, mobile infrastructure, and governance arrangements that facilitate access to digital systems. In Indonesia, this is structured across three levels:

a. Backbone: High-capacity transmission forming the primary national network foundation, raising audit questions about route reliability, long-term capacity, and network resilience.

b. Middle-mile: Infrastructure linking the backbone to distribution points, including satellites for areas lacking terrestrial networks. This poses risks regarding demand forecasting and capacity allocation.

c. Last-mile: Connections for end-users and public facilities, driving audit concerns over accurate location targeting, service quality, and actual usability.

These layers interact dynamically. A highly resilient backbone will not yield inclusive outcomes if last-mile access points are poorly targeted, and satellite capacity will remain underutilized if demand forecasting is inaccurate. Therefore, auditors must assess how these layers seamlessly integrate to support meaningful digital access.

## 2.3 Meaningful Connectivity and Public Value

Meaningful connectivity is achieved when users can access the internet under optimal conditions, at an affordable cost, anytime and anywhere (International Telecommunication Union, n.d.). It spans dimensions like availability, quality, affordability, safety, devices, and digital skills. For instance, a rural health facility may have an internet connection, but frequent outages render telemedicine applications useless.

Connectivity generates public value only when it actively improves lives by enabling access to education, health information, disaster communication, and economic participation. Consequently, an audit focusing solely on physical infrastructure completion misses the critical risks tied to planning, targeting, utilization, and long-term sustainability.

## 3. Institutional Context: Public Telecommunications Infrastructure in Indonesia

Indonesia's universal service policy is designed to close the digital divide by supporting telecommunications development in commercially unattractive areas. As previously noted, BAKTI Komdigi drives this mandate through its backbone (Palapa Ring), middle-mile (SATRIA-1), and last-mile (public internet access and 4G BTS) initiatives.

From a DPI perspective, these programs act as the fundamental enablers for public digital services. A connected school can utilize digital learning platforms; a connected village office can facilitate digital administration. However, executing these large-scale programs introduces complex governance risks, including inaccurate needs assessments, underutilization, weak vendor management, and fiscal exposure. These are not merely technical flaws; they are governance failures that dictate whether public funds truly yield inclusive value. BPK's domestic mandate for evaluating the economy, efficiency, and effectiveness of state financial management makes these lessons highly relevant for the international SAI community and WGITA members dealing with similar technological intersections (BPK RI, 2020; Presiden Republik Indonesia, 2004).

## 4. Methodology

This article utilizes a practice-based case analysis derived from BPK's performance audits of telecommunications infrastructure managed within the BAKTI Komdigi ecosystem. Adhering to standard publication and organizational clearance policies, the analysis abstracts domestic audit experiences into transferable analytical themes suitable for the global SAI community. The analytical framework evaluates backbone infrastructure (for reliability and resilience), middle-mile infrastructure (for demand forecasting and capacity allocation), and last-mile infrastructure (for targeting, service quality, and meaningful access). This approach practically integrates the core tenets of performance auditing, information systems auditing, and inclusive governance to assess whether underserved communities achieve meaningful digital access.

## 5. Audit Risks in the Connectivity Layer of DPI

### 5.1 Targeting and Needs Assessment Risk

Deploying infrastructure without a robust, evidence-based needs assessment creates severe risks of inefficiency and duplication. At the last-mile level, auditors must evaluate whether selected locations truly face service gaps. Locations already served by commercial providers, or those lacking fundamental readiness (such as electricity or devices), indicate poor targeting. Similarly, backbone and middle-mile routes must reflect long-term strategic requirements and realistic demographic distributions. Validating these criteria directly aligns with the efficiency and effectiveness goals outlined in ISSAI 300 and ISSAI 3000 (INTOSAI, 2019e, 2019f).

## 5.2 Capacity Planning and Utilization Risk

Massive investments in bandwidth and satellite capacity do not automatically equate to public value. Capacity must be meticulously aligned with actual and projected demand. If satellite capacity allocations are not based on realistic traffic patterns of the connected public facilities, resources remain underutilized, which is fundamentally a performance governance issue. Auditors should investigate demand forecasting methodologies, how utilization data is monitored, and whether management adjusts allocations based on real-world consumption patterns.

## 5.3 Service Quality and Meaningful Access Risk

A nominal internet connection that is frequently unstable cannot foster digital inclusion (International Telecommunication Union, n.d.). Auditors must scrutinize latency, packet loss, incident frequency, and user complaint resolution times. It is vital to compare reported vendor performance metrics with independent field testing and actual user experiences, as poor service quality outright nullifies the intended governance outcomes of the infrastructure.

## 5.4 Contract Governance and Fiscal Accountability Risk

Telecommunications projects often rely on complex public-private partnerships, service level agreements (SLAs), and availability-based payment structures. A critical audit risk arises if governments pay for sub-standard services due to weak performance verification. Auditors must determine if SLA obligations are enforceable, if performance data is independently verifiable rather than solely vendor-reported, and if financial penalties are appropriately applied for breaches. This domain naturally bridges financial, compliance, and IS audits as outlined in GUID 5100 (INTOSAI, 2019c).

## 5.5 Monitoring, Evaluation, and Performance Data Risk

Monitoring systems that only track physical outputs (e.g., kilometers of fiber laid) fail to capture operational outcomes. Effective systems must track downtime, repair times, and user benefits. Fragmented monitoring data hinders management's ability to take corrective action and jeopardizes fiscal accountability. Auditors should assess the integrity, timeliness, and integration of these monitoring dashboards, ensuring they are utilized for strategic decision-making (INTOSAI, 2019f, 2019a, 2019b).

## 5.6 Sustainability and Resilience Risk

Digital inclusion relies on long-term operational continuity. Infrastructure in remote areas faces extreme weather, geographical constraints, and limited technical expertise. A failure to secure

lifecycle funding, spare parts, and continuous energy supplies will lead to rapid deterioration post-deployment. Auditors must evaluate the existence of continuity plans, network redundancy, and incident response mechanisms to ensure public funds create lasting value.

## 6. Connectivity-Inclusion Governance Audit Framework (CIGAF)

Based on the preceding analysis, this article proposes CIGAF to help SAIs assess whether telecommunications investments genuinely support inclusive governance. Rather than replacing existing frameworks, CIGAF functions as an operational bridge—translating performance and information systems audit principles (SPKN and INTOSAI) into practical audit domains for DPI-enabling infrastructure. As illustrated in Figure 1, CIGAF is designed as an integrated, cyclical model. It emphasizes that technical, financial, and operational domains are deeply interconnected, preventing auditors from rendering a narrow assessment. By guiding evidence collection from the planning to the follow-up stage, CIGAF ensures that findings directly link technical infrastructure vulnerabilities to real-world public value implications.




**Figure 1. The Connectivity-Inclusion Governance Audit Framework (CIGAF)**

To support practical implementation during fieldwork, Table 1 operationalizes these six interconnected domains into specific audit objectives, key questions, and potential sources of evidence.

**Table 1. CIGAF Audit Domains and Operational Matrix**

| CIGAF Domain | Audit Objective | Key Audit Questions | Possible Audit Evidence | Relevance to Inclusive Governance |
|---|---|---|---|---|
| Targeting and Needs Assessment | To determine whether infrastructure is directed to underserved and priority locations | Are location-selection criteria clear and evidence-based? Do selected locations reflect actual service gaps? Is there duplication with commercial services? | Planning documents, coverage maps, public facility data, socioeconomic indicators, geospatial analysis, field verification | Ensures that public investment reaches communities most at risk of digital exclusion |
| Capacity and Utilization | To assess whether infrastructure capacity is aligned with actual and projected demand | Are demand forecasts realistic? Is installed capacity used effectively? Are traffic patterns monitored and used for adjustment? | Traffic data, utilization reports, technical design, capacity dashboards, bandwidth requirement documents | Prevents large infrastructure capacity from failing to generate meaningful benefits |
| Service Quality and Reliability | To evaluate whether connectivity is stable, reliable, and usable | Are service-level standards defined and monitored? Does actual user experience match reported performance? Are outages resolved in a timely manner? | Service Level Agreement (SLA) reports, downtime logs, speed tests, incident reports, user complaints, field testing | Ensures that access is not merely nominal but practically usable |
| Contract Governance and Fiscal Accountability | To assess whether payments and contractual obligations are linked to service performance | Are provider obligations measurable? Are payments verified against reliable performance data? Are penalties or corrective mechanisms applied? | Contracts, payment documents, SLA verification, audit trails, provider reports, performance certificates | Protects public funds and ensures that fiscal commitments generate public value |
| Monitoring and Evaluation | To determine whether management has reliable data on outputs, outcomes, and risks | Are monitoring systems integrated? Do indicators capture operational status, utilization, quality, and benefits? Are monitoring results used for corrective action? | Dashboards, monitoring reports, data governance policies, evaluation reports, management meeting records | Enables government to know whether connectivity contributes to inclusion |
| Sustainability and Resilience | To assess whether infrastructure can provide long-term benefits | Are operations and maintenance planned? Are geographical and security risks mitigated? Are continuity and resilience plans in place? | Operational & maintenance plans, risk registers, continuity plans, incident reports, maintenance budgets | Prevents inclusion gains from deteriorating after deployment |

## 7. Lessons for SAIs and WGITA Members

BPK's experience provides highly transferable audit considerations for SAIs navigating the complexities of modern digital infrastructure:

a. Move beyond physical completion: Audits should actively link infrastructure outputs with utilization and inclusion outcomes, aligning with INTOSAI-P 12's mandate to make a difference in citizens' lives (INTOSAI, 2019d).

b. Prioritize targeting as a core audit issue: SAIs should leverage geospatial data and socioeconomic indicators to verify that investments do not bypass intended beneficiaries.

c. Treat demand forecasting as a performance benchmark: Technical capacity decisions directly dictate efficiency; assumptions must be regularly updated against actual utilization data.

d. Demand verifiable evidence for service quality: Nominal coverage claims are insufficient. Auditors must evaluate latency, downtime, and user incident reports.

e. Strengthen technical contract governance: Evaluating complex SLAs requires ensuring that payments are strictly tethered to verified service delivery, not merely administrative checklists.

f. Demand outcome-oriented monitoring: Management dashboards must track whether services are working and benefiting users, rather than simply counting deployed assets.

g. Cultivate multidisciplinary audit teams: Assessing DPI-enabling networks requires blending public finance, telecommunications, data analytics, and policy evaluation expertise.

h. Frame audit communications around public value: Technical findings resonate best with legislatures and society when translated into tangible implications for public trust and service delivery.

## 8. Discussion and Conclusion

While telecommunications infrastructure shares a deeply symbiotic relationship with DPI, it is vital to maintain a conceptual distinction. Framing BAKTI Komdigi's initiatives strictly as the connectivity layer offers a precise, empirically grounded middle path. It avoids an overly platform-centric agenda that turns a blind eye to fundamental access barriers, while aligning seamlessly with Indonesia's National Digital Transformation Index, which positions network infrastructure as the preliminary foundational stage required before digital adoption can occur (Kementerian Komunikasi dan Digital, 2024).

Digital public infrastructure possesses immense potential to democratize governance, yet this potential remains locked unless citizens possess reliable, affordable connectivity. BPK's audit experiences demonstrate that scrutinizing this connectivity layer requires auditors to transcend basic deployment verification. The proposed Connectivity-Inclusion Governance Audit Framework (CIGAF) equips SAIs with a structured methodology to bridge technical IT audits with public sector performance standards.

Ultimately, as governments globally accelerate their digital transitions, the paramount question for SAIs is not merely whether digital infrastructure was built, but whether it actively and sustainably improves the lives of the citizens it was intended to serve.

## References

BAKTI. (2023, October 24). *BAKTI Kominfo Berkomitmen Percepat Transformasi Digital Melalui Perbaikan Tata Kelola Organisasi*. https://baktikomdigi.id/id/detail-berita/bakti-kominfo-berkomitmen-percepat-transformasi-digital-melalui-perbaikan-tata-kelola-organisasi

BAKTI. (2024, October 18). *Keberhasilan Tugas Satgas BAKTI Kominfo di Masa Akhir Penugasan dari Menkominfo*. https://baktikomdigi.id/index.php/id/detail-berita/keberhasilan-tugas-satgas-bakti-kominfo-di-masa-akhir-penugasan-dari-menkominfo

BPK RI. (2020, April 19). *Jenis Pemeriksaan BPK*. https://www.bpk.go.id/news/jenis-pemeriksaan-bpk

Clark, J., Marin, G., Ardic Alper, O. P., & Galicia Rabadan, G. A. (2025). *Digital Public Infrastructure and Development: A World Bank Group Approach*. Washington, DC: World Bank. https://doi.org/10.1596/42935

Fetter, J., Rao, K., & Eaves, D. (2025). *2025 State of Digital Public Infrastructure Report: A Look at Measurement and Prevalence as DPI Transitions from Experiment to Scale*. UCL Institute for Innovation and Public Purpose. https://www.ucl.ac.uk/bartlett/publications/2025/nov/2025-state-digital-public-infrastructure-report

International Telecommunication Union. (n.d.). *About universal and meaningful connectivity*.

Retrieved https://www.itu.int/itu-d/sites/projectumc/home/aboutumc/

INTOSAI. (2019a). *GUID 3910: Central concepts for performance auditing. International Organization of Supreme Audit Institutions*. https://www.issai.org/pronouncements/guid-3910-central-concepts-for-performance-auditing/

INTOSAI. (2019b). *GUID 3920: The performance auditing process. International Organization of Supreme Audit Institutions*. https://www.issai.org/pronouncements/guid-3920-the-performance-auditing-process/

INTOSAI. (2019c). *GUID 5100: Guidance on audit of information systems*. https://www.issai.org/pronouncements/guidance-on-audit-of-information-systems/

INTOSAI. (2019d). *INTOSAI-P 12: The value and benefits of Supreme Audit Institutions—Making a difference to the lives of citizens*. https://www.issai.org/pronouncements/intosai-p-12-the-value-and-benefits-of-supreme-audit-institutions-making-a-difference-to-the-lives-of-citizens/

INTOSAI. (2019e). *ISSAI 300: Performance audit principles. International Organization of Supreme Audit Institutions*. https://www.issai.org/pronouncements/issai-300-performance-audit-principles/

INTOSAI. (2019f). *ISSAI 3000: Performance audit standard. International Organization of Supreme Audit Institutions*. https://www.issai.org/pronouncements/issai-3000-performance-audit-standard/

Kementerian Komunikasi dan Digital. (2024). *Indeks Transformasi Digital Nasional: Pocket Book*

OECD. (2024). *Digital public infrastructure for digital governments* (68th ed., OECD Public Governance Policy Papers) [OECD Public Governance Policy Papers]. https://doi.org/10.1787/ff525dc8-en

Presiden Republik Indonesia. (2004). *Undang-Undang Nomor 15 Tahun 2004 tentang Pemeriksaan Pengelolaan dan Tanggung Jawab Keuangan Negara*.

United Nations. (n.d.). *Digital Public Infrastructure*. Retrieved https://www.undp.org/digital/digital-public-infrastructure

United Nations. (2024a). *Global Digital Compact*. https://www.un.org/global-digital-compact United Nations. (2024b). *United Nations E-Government Survey 2024: Accelerating digital transformation for sustainable development*. https://publicadministration.un.org/egovkb/en-us/reports/un-e-government-survey-2024

United Nations. (2024c). *Universal DPI Safeguards Framework: A Guide to Building Safe and Inclusive DPI for Societies*. https://framework-dpi-safeguards.org/frameworkpdf

United Nations. (2024d, September 24). *UN Releases Universal DPI Safeguards Framework to Promote Safe and Inclusive Digital Public Infrastructure*. https://www.undp.org/press-releases/un-releases-universal-dpi-safeguards-framework-promote-safe-and-inclusive-digital-public-infrastructure

United Nations Development Programme. (2023). *The DPI Approach: A Playbook*. United Nations Development Programme (UNDP). https://www.undp.org/publications/dpi-approach-playbook

World Bank Group. (2025). *Digital Public Infrastructure and Development: A World Bank Group Approach*.

https://documents1.worldbank.org/curated/en/099031025172027713/pdf/P505739-84c5073b-9d40-4b83-a211-98b2263e87dd.pdf

# Digital Public Infrastructure and Cloud Computing: GAO Identified Challenges

**Jonnie Genova & Jess Lionne**
U.S. Government Accountability Office (GAO)





## Abstract

Cloud services are a core element of digital public infrastructure. Increasing government efficiency while keeping citizens connected is a responsibility that includes the use of cloud services. GAO's body of work highlights challenges related to the federal government's adoption of cloud services and related recommendations for improvement.

## Keywords

Cloud, government, digital, infrastructure, cybersecurity.

Increasing government efficiency while keeping citizens connected and secure is a responsibility for governments on a global scale. An essential component of this responsibility includes digital public infrastructure (DPI). DPI is a locus of modern societies, offering communication and connection between people and governments. Much like other critical infrastructure systems such as water, roadways, and transportation, digital infrastructure offers access to essential systems that shape modern living. Well-designed DPI can be used in numerous ways that benefit citizens, including delivering essential services, creating economic opportunities, facilitating secure banking, and the distribution of social benefits.

The continued rise in DPI highlights the need for collaboration between government and private entities. Increased collaboration and the exchange of ideas will be key in overcoming challenges and advancing strategies to allow for the adoption of DPI on a global scale. The successful use of DPI must hinge on inclusivity and consideration of the greater good.

Cloud computing is a critical element of DPI that offers significant opportunities to increase government efficiency, as well as benefits for the public in accessing a secure digital infrastructure of publicly available services. The United States (U.S.) federal government has

recognized these benefits and is increasingly using cloud computing services to access shared resources such as networks, servers, and data storage. The U.S. Government Accountability Office (GAO) has reported on ways that U.S. government agencies use cloud computing to procure services more quickly and at a lower cost than building, operating, and maintaining these computing resources themselves.

Recent examples include:

- A government agency that moved its system to the cloud enhanced its information sharing and collaboration capabilities, enabling it to respond more effectively to major national events like hurricanes.
- Another agency used cloud computing to replace multiple aging IT systems that manage its daily business activities, such as processing payments.
- An agency used cloud to consolidate case management systems that are used to interact with the U.S. workforce and retirees.
- An agency used cloud to improve how it stores and manages documentation used to help manage federal lands.

But a cloud infrastructure that addresses global challenges by providing services in areas like social security, health, education, travel, and finance is also vulnerable to cybersecurity threats. Cloud services used by both government and private sector organisations require a comprehensive framework of safeguards to prevent unintended negative consequences.

GAO's work highlights challenges related to the U.S. federal government's adoption and use of cloud services and includes recommendations for procuring and utilizing these services in a secure way. These challenges, while multiple, include ensuring cybersecurity and procuring cloud services.



Source: alice_photo/stock.adobe.com.

## Ensuring Cybersecurity in Cloud Adoption

One of GAO's latest reports on cloud computing looked at how some U.S. government agencies protect data in the cloud when contracting with providers for cloud services. As government data includes the personal information of millions of people, as well as sensitive and confidential information, the use of cloud computing poses security risks. These risks arise when agencies and cloud service providers do not effectively implement security controls over their cloud services. Weaknesses in these controls could lead to vulnerabilities affecting the confidentiality, integrity, and availability of information stored and shared in the cloud. Working with cloud service providers to effectively implement information security controls is a vital part of reducing these risks.

GAO's recent audit found that government agencies varied in their efforts to implement and ensure compliance with three key cloud security practices when contracting with cloud service providers. These practices include **continuous monitoring**, **incident response and recovery**, and **service level agreement (SLA) implementation**.

In particular, three of the four government agencies that we selected for audit had one or more systems with shortfalls in implementing continuous monitoring, documenting incident response and recovery procedures, and properly defining service level agreements.

Fully implementing key cloud security practices will help address a number of increased risks and keep cloud data safe. For example, implementing key practices associated with continuous monitoring allows entities to promptly detect unauthorized access attempts or anomalous activity, protecting critical systems and data from compromise. Additionally, clearly defined and tested incident response and recovery procedures better position government agencies to detect, contain, and remediate cyber threat events. High-profile cyber incidents like the SolarWinds and Microsoft Exchange attacks underscore the threats that U.S. federal agencies and service providers face in ensuring proper incident response and recovery. Incidents such as these have occurred in numerous locales and are likely to continue and even increase. Furthermore, without robust incident recovery protocols, agencies may not be able to ensure that recovery activities are effective. Additionally, without properly defined service level agreements, agencies may not receive the services they require or be able to hold providers accountable if service levels fall below expectations.

GAO's recommendations in this audit included that agencies should ensure compliance and implementation with the three key cloud security practices when contracting with cloud service providers. Doing so will address a number of increased risks.

## Procuring Cloud Services

Government agencies need to maximize the impact of taxpayer dollars and make procurement decisions that deliver on their missions securely and reliably. These investments also have the

potential to make agencies more efficient in fulfilling their missions by reducing costs and improving operational efficiencies. Cloud computing is a means for enabling on-demand access to shared pools of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released. Cloud services offer federal agencies a means to buy services more quickly and possibly at a lower cost than building, operating, and maintaining these computing resources themselves.

For more than a decade, GAO has reported on federal agencies' efforts to implement cloud services and the challenges they have identified with these efforts. Our recent audit determined that of 24 government agencies, 22 reported primarily relying on historical procurement data to help make cloud decisions. Timely implementation of the many recommendations GAO has made to federal agencies to improve these data could result in better quality information.

Our report showed that agencies also faced challenges in controlling cloud costs, obtaining authorized cloud solutions, and responding to cloud staffing limitations. Agencies' ongoing and planned actions, if implemented effectively, demonstrate promise for tackling these challenges and could lead to substantial savings for both government and the taxpayer.

In contrast, our report also noted that the challenges of conflicting software guidance, outdated federal acquisition regulations, and multi-vendor cloud solutions remain. Specifically, conflicting guidance has created unnecessary burdens for collecting and storing key software components. Moreover, GAO's audit highlighted the importance of a clearly stated definition of cloud computing, as well as ensuring that acquisition regulations reflect present day computing needs as essential to effectively contracting for cloud services.

Our report also found that, while several larger government agencies are using multiple cloud vendors to achieve efficiencies, they are also experiencing new technical challenges such as interoperability among cloud service platforms. Sharing multi-cloud leading practices would enable other agencies to learn from each other and improve implementation efforts.

Other challenges also hamper federal agencies' pursuit of cloud solutions. Agencies continue to struggle with managing their cloud costs. One agency's financial operations pilot—also known as FinOps—demonstrated that agencies could optimize their cloud environments to improve service operability, increase security, and identify cost savings. Expanding the FinOps framework across the federal government could lead to substantial cost savings.

GAO's recommendations in this audit included that Congress should consider requiring changes to federal acquisition regulations to update cloud-related definitions, and that agencies need to address cloud cost management practices, conflicting cloud guidance, and multi-vendor cloud solutions.

Agencies and organizations are faced with the need to accelerate the adoption of cloud services, while also ensuring the systems that support their missions are safe and secure when operating in the cloud. But effective implementation of cloud security and ensuring the protection of data

maintained in the cloud is key. Additionally, addressing challenges related to controlling cloud costs and addressing issues with cloud procurement can help agencies and government in the adoption of cloud services. GAO's recent audits highlight the ways in which adoption of cloud services can be done safely and effectively, while keeping citizens and governments connected. The successful adoption of cloud services is a fundamental component of inclusive DPI.




Section III

# DPI IN THE SECTORS: SERVICE DELIVERY ON THE GROUND

# AgniDrishti: An AI-Enabled Fire Risk Intelligence System as Digital Public Infrastructure for India's Fire and Emergency Services



**Tania Mishra**
O/o the Comptroller & Auditor General of India

## Abstract

India's fire and emergency services departments collect geo-tagged incident data, building registration records, and appliance deployment logs at scale, yet no state fire department operates an integrated system that converts this data into predictive risk intelligence. Five successive Comptroller & Auditor General of India (CAG) audit reports West Bengal (2019), Himachal Pradesh (2022), Tamil Nadu (2022-23), Maharashtra Urban Local Bodies (2016), and the West Bengal Fire and Emergency Services Subject Specific Compliance Audit (SSCA, 2023-26), document structurally identical deficiencies: chronic station shortfalls, vacant posts, dysfunctional hydrant networks, and the complete absence of risk-profiling or analytical systems. This article argues that the recursive pattern of findings reflects a structural gap in the standard recommendation taxonomy: departments are directed toward analytical outcomes such as vulnerability surveys andrisk profiles without being prescribed the digital infrastructure capable of producing and sustaining them. Framing the problem through the Digital Public Infrastructure (DPI) paradigm emphasizing open, interoperable, government-grade digital systems that convert siloed administrative data into shared governance intelligence the article introduces AgniDrishti ('Fire Vision'), a working AI-assisted fire risk analysis prototype built during the West Bengal Fire and Emergency Services (WBFES) SSCA field posting. The article details AgniDrishti's six-module architecture, its Composite Risk Index (CRI) algorithm drawing on six categories of government-authoritative data, and its technology stack engineered for zero-licensing-cost deployment on National Informatics Centre (NIC) cloud infrastructure. It proposes the AI-enabled Fire Risk Identification and Resource Allocation System (AFIRAS) as a Level 2 INTOSAI-framework recommendation for SSCA reports on fire services, grounded in technical demonstration rather than specification alone.

## Keywords

Digital Public Infrastructure, Composite Risk Index, fire safety audit, AI in public governance, Supreme Audit Institutions, AgniDrishti

## 1. INTRODUCTION

India's Digital Public Infrastructure achievements, including Aadhaar's biometric identity layer, UPI's interoperable payments stack, CoWIN's vaccine delivery platform share a common architectural logic: open-standard systems deployed on national technology infrastructure, converting what government agencies already collect into actionable shared intelligence. The data is not new; the architecture that integrates and activates it is. This principle is the template on which fire governance reform must be built.

Fire and emergency services have not benefited from this DPI trajectory. India's state fire departments collect operational data at scale: geo-tagged incident records, building registration files, appliance deployment logs, hydrant network maps, and census-linked population data. The governance gap is not a data deficit. It is an architecture deficit: no state fire department operates an integrated system that converts existing data into predictive risk intelligence.

The Comptroller and Auditor General of India has documented this architecture deficit, with technical rigour, across five audit cycles in four states. The pattern is structurally identical in each: the audit correctly identifies the absence of a vulnerability survey, a risk profile, an analytical system; recommends that the department produce one; the department, lacking both the system and the staffing to manually sustain one, does not; and the next audit cycle finds substantially the same situation.

This article argues that the DPI framework provides both the conceptual template and the institutional vocabulary for a qualitatively different class of recommendation, one that prescribes the analytical architecture, not merely the analytical outcome. It introduces AgniDrishti (Fire Vision), a working prototype built entirely on open-source components during field posting for the WBFES SSCA, as technical demonstration that such a recommendation is feasible. The governing premise is this: if five successive audit reports have established that the gap exists, the next engagement must propose the infrastructure capable of closing it.

## 2. THE RECURRING AUDIT RECORD: THREE STRUCTURAL FINDINGS

### 2.1 West Bengal: CAG Report No. 4 of 2019

The CAG's Report on the General and Social Sector, West Bengal (CAG, 2019a), documented a 60 per cent shortfall in fire stations against population norms (173 operational against a required 435), a 73 per cent vacancy rate in control room posts (31 of 116 sanctioned posts filled), non-

functional fire hydrants in 15 of 24 divisions, and the complete absence of a systematic fire vulnerability survey. The principal recommendation directed the Department to conduct a comprehensive survey of fire-prone areas, industrial zones, and high-rise buildings to identify vulnerability. Seven years later, the West Bengal SSCA (PAG Audit-I, 2026) found the same station shortfall, the same vacancy rate, and no analytical system in operation.

The structural failure is not non-compliance alone; it is recommendation design. A one-time survey produces a static snapshot of a dynamic phenomenon. Fire risk evolves continuously with incident accumulation, seasonal conditions, building development, and industrial expansion. A recommendation that asks for a survey asks for an instrument technically inadequate to the variable it is intended to measure.

## 2.2 Himachal Pradesh: CAG Report No. 3 of 2022

The CAG's compliance audit of fire services preparedness in Himachal Pradesh (CAG, 2022) found that against 115 approved firefighting vehicles, only 85 were operational with 32 having exceeded their condemnation age. Across all 23 test-checked fire control centres, no adequate and reliable water source existed. A budget of Rs. 6.22 crore earmarked for vehicle procurement during 2018-21 was surrendered through inadequate planning. Most significantly, the report found that the Department had not conducted vulnerability analysis of fire vulnerable buildings and had not prepared a database of hazardous industries (CAG, 2022, Chapter IV, p. 37) the identical finding that the Public Accounts Committee had made following the prior audit cycle in 2016. The Department attributed non-compliance to staff shortage.

This attribution reveals the structural problem with precision. The Department had no system capable of maintaining a vulnerability database without dedicated manual labour. Manual maintenance requires permanent staff allocation. Staff shortage means the database cannot be built or sustained. The cycle is closed and self-reinforcing. A system recommendation would break it by making database maintenance automatic independent of staffing levels.

## 2.3 Tamil Nadu: CAG Report No. 5 of 2023

The CAG's compliance audit of Tamil Nadu's Fire and Rescue Services covering 2017-22 (CAG, 2023) found 352 stations against a calculated requirement of 451, representing a 22 per cent shortfall concentrated in the rural districts recording the highest incident rates. The Department had neither conducted any vulnerability analysis nor fixed the staff component based on risk profile (CAG, 2023, p. 47), despite the National Disaster Management Authority (NDMA) Guidelines (2012) having mandated risk-profile-based staffing norms since 2012 an eleven-year non-compliance gap. Sanctioned strength of 17 personnel per station had not been revised since the 1970s. Rs. 4.73 crore for water tenders was surrendered unreleased.

The resource allocation pattern is diagnostically important. In the absence of a risk-profile system, resource deployment defaults to historical administrative demarcation rather than incident geography. The result is that the highest-risk districts are the least resourced precisely because no system has classified and quantified them as high-risk. This is the gap a CRI-based engine directly and continuously addresses.

## 2.4 The Structural Gap

A cross-reading of these three reports alongside the Maharashtra Urban Local Bodies audit (CAG, 2016) and the WBFES SSCA (PAG Audit-I, 2026) establishes a single structural gap: every report recommends that the department produce a vulnerability analysis and risk profile; none recommends the analytical architecture capable of generating and continuously updating that profile. Table 1 maps each report's core technical deficiency to the AgniDrishti module that directly addresses it.

**Table 1: CAG Audit Finding and AgniDrishti Capability Mapping**

| CAG Report | Core Technical Deficiency Documented | AgniDrishti Module and Capability |
|---|---|---|
| WB 2019 (CAG, 2019a) | Complete absence of fire vulnerability survey; 60% station shortfall (173/435 operational); 73% control room vacancy (31/116 posts); non-functional hydrants in 15/24 divisions | Modules 2 and 4 (Predictive + Heat Map): CRI recomputed continuously from geo-tagged incident data; dynamic vulnerability map updated with every new record no periodic survey required |
| HP 2022 (CAG, 2022) | No vulnerability analysis of buildings; no database of hazardous industries; Rs. 6.22 crore budget surrendered; non-compliance finding identical to prior PAC recommendation (2016) | Module 2 and CRI Engine: AI-maintained geo-tagged database drawing on building census, NBC 2016 classifications, and Hazardous Chemical Rules 1989 safe-distance thresholds |
| TN 2023 (CAG, 2023) | No risk-profile-based staffing despite NDMA mandate (2012); station shortfall concentrated in highest-incident rural districts; Rs. 4.73 crore water tender allocation surrendered | CRI Engine: Multi-dimensional composite risk score at station level. Module 3 (Responsive): NDMA-calibrated personnel deployment minor: 4; major: 50; critical: 100 personnel |
| Maharashtra ULBs 2016 (CAG, 2016) | Periodical inspections of high-rise and dilapidated buildings not conducted; no data analytics for inspection scheduling; enforcement entirely discretionary | Module 5 (Inspection Priority Queue): ML-assisted ranking by NBC 2016 building group (A-J), occupancy type, proximity to high-CRI zones, and historical incident density |
| WBFES SSCA 2023-26 (PAG Audit-I, 2026) | Rs. 216.75 crore of 15th FC modernisation grant unclaimed; 40,433 geo-tagged incidents; 98 fatalities; no evidence-based infrastructure investment plan | Module 6 (Investment Map): Marginal response-time analysis generating ranked investment priorities stations and appliance positions that most reduce predicted response time |

*Source: CAG (2016, 2019a, 2022, 2023); PAG Audit-I (2026); AgniDrishti prototype (author).*

# 3. AGNIDRISHTI: TECHNICAL ARCHITECTURE

AgniDrishti is a working prototype of an AI-assisted fire risk analysis and decision-support system built entirely on open-source components during field posting for the WBFES SSCA. It requires no proprietary APIs, no paid services, and no institutional resources beyond what NIC's existing cloud infrastructure already provides. It comprises six integrated modules, a rule-based analytical engine architected for ML upgrade, and a data layer grounded exclusively in government-authoritative sources.

## 3.1 Data Architecture

AgniDrishti's analytical outputs derive their credibility from a data architecture grounded in six categories of government-authoritative, open-access sources. Table 2 details the categories,

primary sources, and system function for each. The traceability of every standard embedded in the system is a deliberate design decision, not a technical convenience.

The NDMA (2012) response-time benchmarks urban: 5-7 minutes; semi-urban: 10-15 minutes; rural: 20-30 minutes are embedded in the responsive mode engine not as estimates but as government-mandated benchmarks, directly citeable in audit observations. The National Building Code (NBC) of India 2016 Part 4 building group classification, covering Groups A through J, from Residential to Hazardous drives the inspection priority queue not as a design heuristic but as a published statutory classification. The Hazardous Chemical Rules, 1989 safe-distance thresholds (500 metres from residential areas; 1,000 metres from schools and hospitals) power the secondary hazard risk dimension not as a proxy but as a legally enforceable norm. This evidentiary chain transforms AgniDrishti's outputs from algorithmic estimates into government standards applied to government data the feature that makes every output audit-defensible and verifiable in action-taken reports.

**Table 2: AgniDrishti Data Architecture Categories, Sources, and System Function**

| Data Category | Primary Source(s) | Function in AgniDrishti |
|---|---|---|
| Demographics | Census of India 2011; SRS 2020 (Office of the Registrar General) | Population density and urbanisation rates primary input to Human Life Risk (H) dimension of CRI; determines alert priority in densely populated and institutionally concentrated areas |
| Fire Safety Standards | NBC 2016 Part 4 (IS SP 7:2016); IS 15683:2006; NDMA Guidelines 2012; SFAC Norms 2018 | Building group classification (Groups A-J); fire class taxonomy (Classes A-F); response-time benchmarks (urban: 5-7 min; semi-urban: 10-15 min; rural: 20-30 min); personnel and water minima by severity level |
| Industrial and Hazardous Areas | Hazardous Chemical Rules 1989 (amended 2000); DPIIT Industrial Data 2023; ASI 2021; Factories Act 1948 s.38 | Industrial zone mapping; safe-distance thresholds (500 m from residential areas; 1,000 m from schools and hospitals) input to Secondary Hazard Risk (S) dimension of CRI |
| Forest and Environment | ISFR 2021 (FSI); NAPFF 2018 (MoEFCC); NASA FIRMS (MODIS/VIIRS) 2024 | Forest cover and fire-prone zone data; regional fire season windows (Northern India: Feb-Jun; NE India: Oct-Mar; Deccan: Mar-May); satellite active-fire detection input to Environmental Risk (E) and seasonal CRI calibration |
| Geospatial and Mapping | Survey of India boundaries (DST); OpenStreetMap + Nominatim; Bhuvan/NRSC 2023 (ISRO); Esri World Imagery (open tile) | Base map tiles; auto-geocoding from caller or typed location; satellite imagery for terrain analysis; coordinate reference framework; fire spread radius computation inputs |
| Electrical Safety | Indian Electricity Rules 1956; CEA (Safety and Electric Supply) Regulations 2010 | Electrical fire (IS Class E) risk norms; transformer and wiring safety benchmarks used in building-level risk scoring for the inspection priority queue |

*Note: All data sources are publicly available, government-authoritative, and free of licensing constraints.*
*Source: Author.*

## 3.2 The Composite Risk Index Algorithm

The analytical core of AgniDrishti is the Composite Risk Index (CRI), computed for each geographic unit on a continuous scale of 0-100 across four independently scored dimensions.

**Human Life Risk (H)** integrates Census 2011 population density (persons/km²) at block level, weighted proximity of schools and hospitals from OpenStreetMap records, and residential concentration from SRS 2020 urbanisation data. It captures the vulnerability of human life in the event of fire, determining alert priority in densely populated and institutionally concentrated areas.

**Property Damage Risk (P)** processes building density, floor area ratio, construction type, building age, and NBC 2016 Part 4 group classification weighted from Group A (Residential) through Group J (Hazardous) to assess economic and structural exposure. Group J buildings carry the

highest property risk weight; scoring is applied per block unit against the NBC group distribution in that unit.

**Environmental Risk (E)** draws on Forest Survey of India (FSI, 2021) cover data, National Action Plan on Forest Fires (NAPFF) (Ministry of Environment, Forest & Climate Change (MoEFCC), 2018) fire season calendars, and NASA FIRMS (2024) active-fire detection points to quantify ecological vulnerability calibrated to regional seasonality: Northern India February-June; North-Eastern India October-March; Deccan Plateau March-May.

**Secondary Hazard Risk (S)** applies the Hazardous Chemical Rules 1989 safe-distance thresholds to proximity data for fuel stations, chemical storage facilities, and industrial installations from Department for Promotion of Industry and Internal Trade (DPIIT), (2023) to capture incident escalation probability from hazardous material adjacency.

The four dimension scores are aggregated with configurable dimension weights default configuration: H = 30%, P = 25%, E = 20%, S = 25% into the composite CRI value:

$$CRI = (0.30 \times H) + (0.25 \times P) + (0.20 \times E) + (0.25 \times S)$$

The resulting CRI is rendered on a five-tier scale Low (0-20), Moderate (21-40), Elevated (41-60), High (61-80), Critical (81-100) and drives three downstream operational modules: the heat map visualisation, the inspection priority queue, and the infrastructure investment map. Dimension weights are configurable by the department or NIC to reflect state-specific risk and seasonal profiles.

## 3.3 The Six Operational Modules

**Module 1: Hierarchical Navigation Dashboard** mirrors India's administrative hierarchy National to State to District to Block/Fire Station presenting live metrics calibrated to each actor's decision-making scale: active fires, deployed personnel, appliances in service, high-risk zones exceeding alert threshold, and pending inspections. The State Fire Controller sees the state-level risk map; the Station Officer accesses the incident reporting and resource recommendation interface.

**Module 2: Predictive Mode** continuously recomputes CRI values from the four-dimensional data layer, generating a dynamic fire vulnerability map updated with every new incident record submitted to the platform. This is the comprehensive vulnerability survey that three successive CAG reports recommended be conducted continuously, automatically, and without additional staffing requirements.

**Module 3: Responsive Mode** processes a submitted incident report specifying location (auto-geocoded from caller data or manual entry), fire class under Indian Standard (IS) 15683:2006 (Structure, Vegetation, Vehicle, Industrial, Electrical, Chemical/Hazmat), and severity level to generate pre-departure field outputs: predicted spread radius from severity, building density,

terrain gradient, and NAPFF seasonal wind indicators; critical assets within the predicted radius; equipment specification calibrated to fire class and NDMA severity benchmarks; personnel count by role (minor: 4; moderate: 8; significant: 20; major: 50; critical: 100); and nearest available appliances with estimated arrival time.

**Module 4: Fire Risk Heat Map** provides a continuous, toggleable visualisation of fire risk intensity derived from geo-tagged historical incidents weighted by CRI. The map updates with every submitted incident record, converting zones of chronic fire concentration into an immediately actionable spatial priority map for inspection scheduling, appliance pre-positioning, and infrastructure investment planning.

**Module 5: Fire Safety Registration and Inspection Priority Queue** ingests Fire Safety Registration data, scores buildings by NBC 2016 Part 4 group classification, occupancy type, proximity to high-CRI zones, and historical incident density, and generates a ranked ML-assisted inspection queue. This converts the discretionary inspection schedule that the Maharashtra CAG (2016) found non-functional into a data-driven, auditable priority list every ranking traceable to a published statutory classification.

**Module 6: Infrastructure Investment Map** applies marginal response-time analysis to the geo-tagged incident database to generate a ranked investment priority list: locations at which a new fire station produces the greatest reduction in predicted response time; divisions where appliance pre-positioning most reduces predicted fire spread; water source gaps most correlated with incident severity in high-CRI zones. This converts the 15th Finance Commission modernisation grant utilisation requirement (Rs. 216.75 crore unclaimed in West Bengal as at 2026) from a compliance obligation into an evidence-based investment plan.

**Table 3: AgniDrishti Technology Stack Government Deployability Assessment**

| Layer | Technology | Government Deployability Rationale |
|---|---|---|
| Backend | Node.js + Express.js | Open-source; zero licensing cost; widely deployed in NIC environments; large Indian developer community ensures long-term maintainability |
| Mapping | Leaflet.js + OpenStreetMap + Nominatim | Open-source; offline-capable; compatible with government geospatial data standards; no third-party API dependency or recurring usage cost |
| Satellite Imagery | Esri World Imagery (open tile layer) | High-resolution imagery without API key or subscription fee; supports both rural and urban terrain analysis for fire spread radius computation |
| Analysis Engine | Rule-based JS modules (ML-upgradeable) | Deterministic logic with a clear, auditable decision trail; designed for direct upgrade to machine-learning pipelines as incident data accumulates to training-scale volumes |
| Data Layer | Structured JSON / PostgreSQL-portable | Portable to NIC GeM-standard PostgreSQL/PostGIS database; no proprietary data format; interoperable with existing government data infrastructure and state FRS portals |
| Build Tool | Vite (open-source) | Lightweight bundler with no vendor dependency; standard for modern government web applications on NIC infrastructure |
| Infrastructure | NIC Cloud (NICSI) / MeitY Digital India | Existing government cloud infrastructure; operational under the Digital India framework; no new capital procurement required for production deployment |

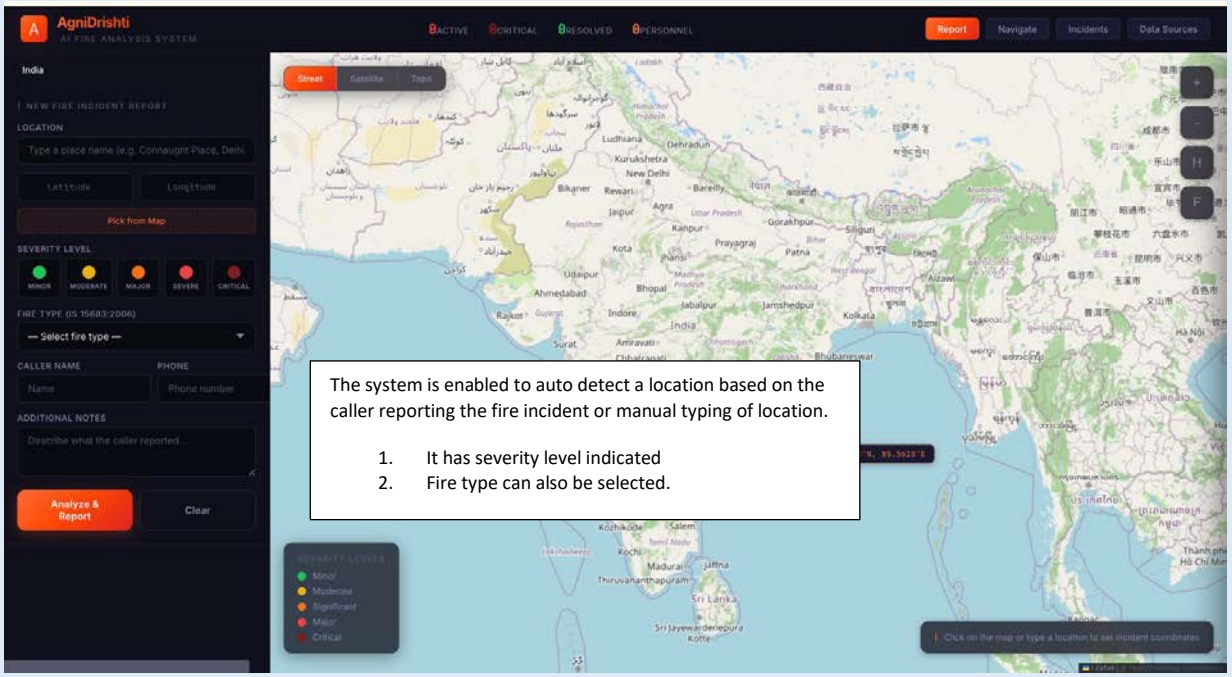
*Note: All components are open-source and deployable on NIC NICSI cloud infrastructure under MeitY's/Digital India framework without capital procurement. Source: Author.*

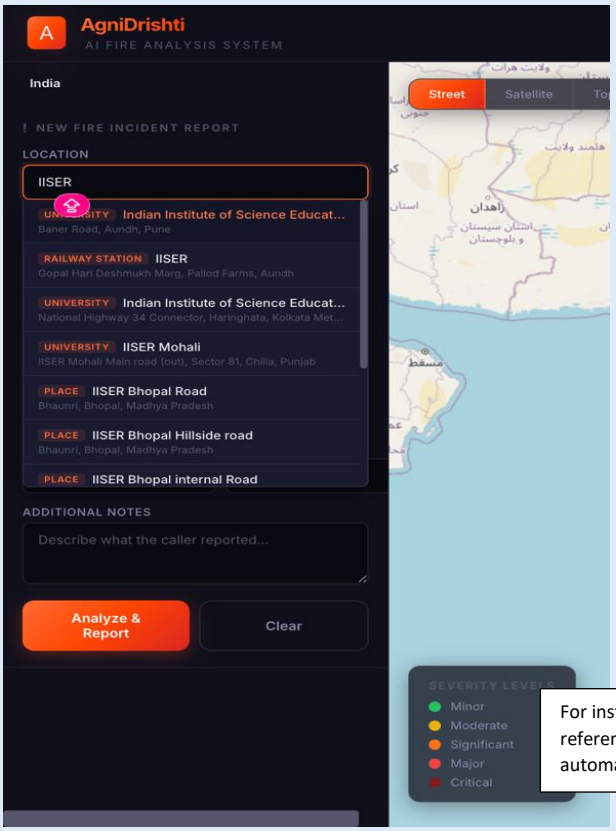
## 3.4 Technology Stack and Government Deployability

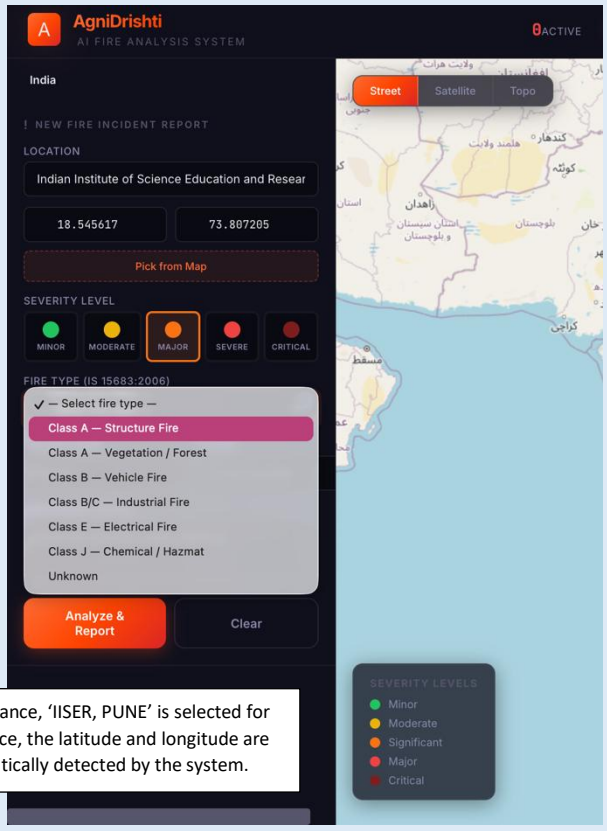
Every component in AgniDrishti's technology stack was selected against a single binding constraint: deployability on NIC cloud infrastructure without new procurement, vendor dependency, or licensing cost. Table 3 sets out the full stack against this deployability criterion.

The prototype was built on a personal computing environment during field posting without institutional resources. The National Informatics Centre with dedicated engineering resources, established data ingestion pipelines, and National Informatics Centre Services Inc. (NICSI) cloud infrastructure can build the production system.

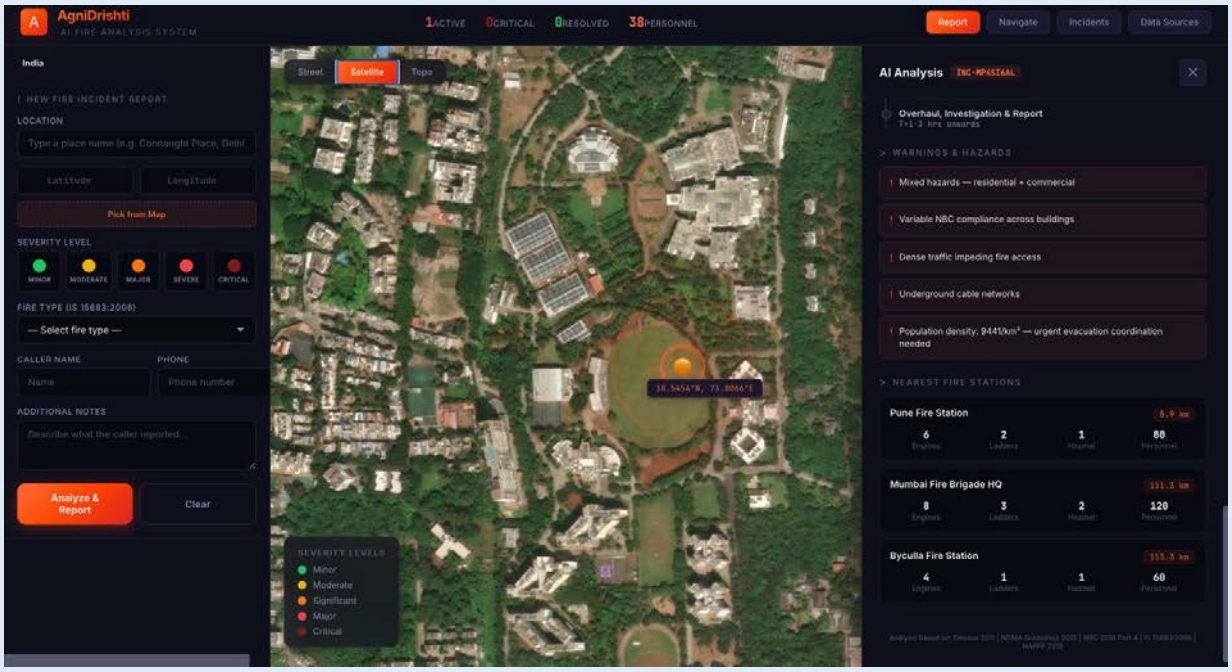
**AGNIDRISHTI - SNAPSHOTS**



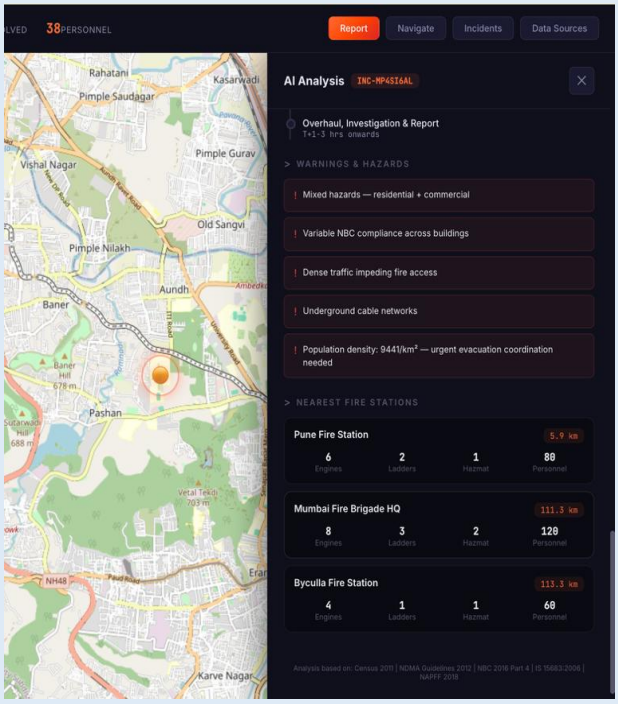



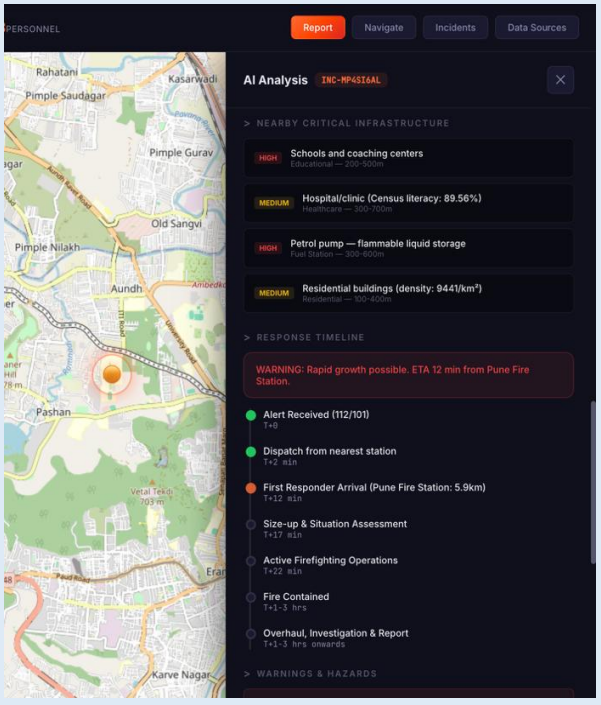




For instance, 'IISER, PUNE' is selected for reference, the latitude and longitude are automatically detected by the system.

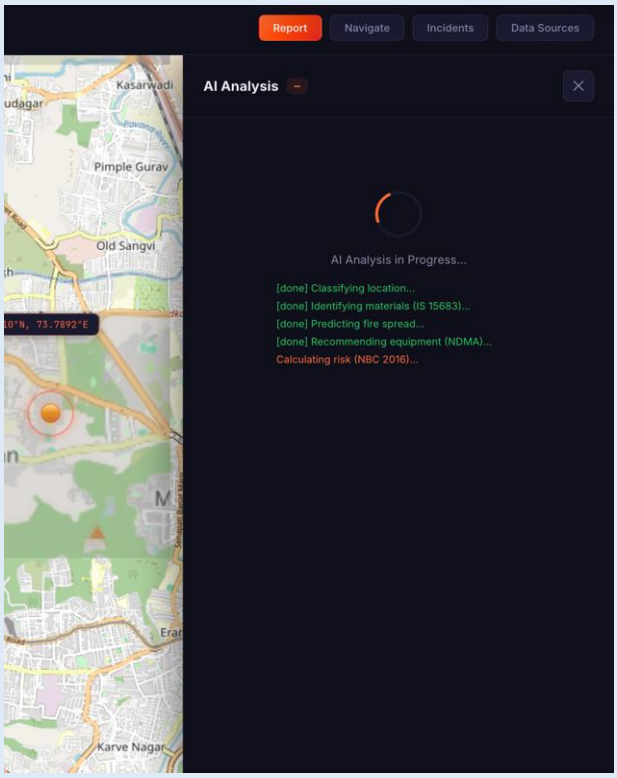



3. Analysis also incudes- nearby critical infrastructure, alert time, response time etc.



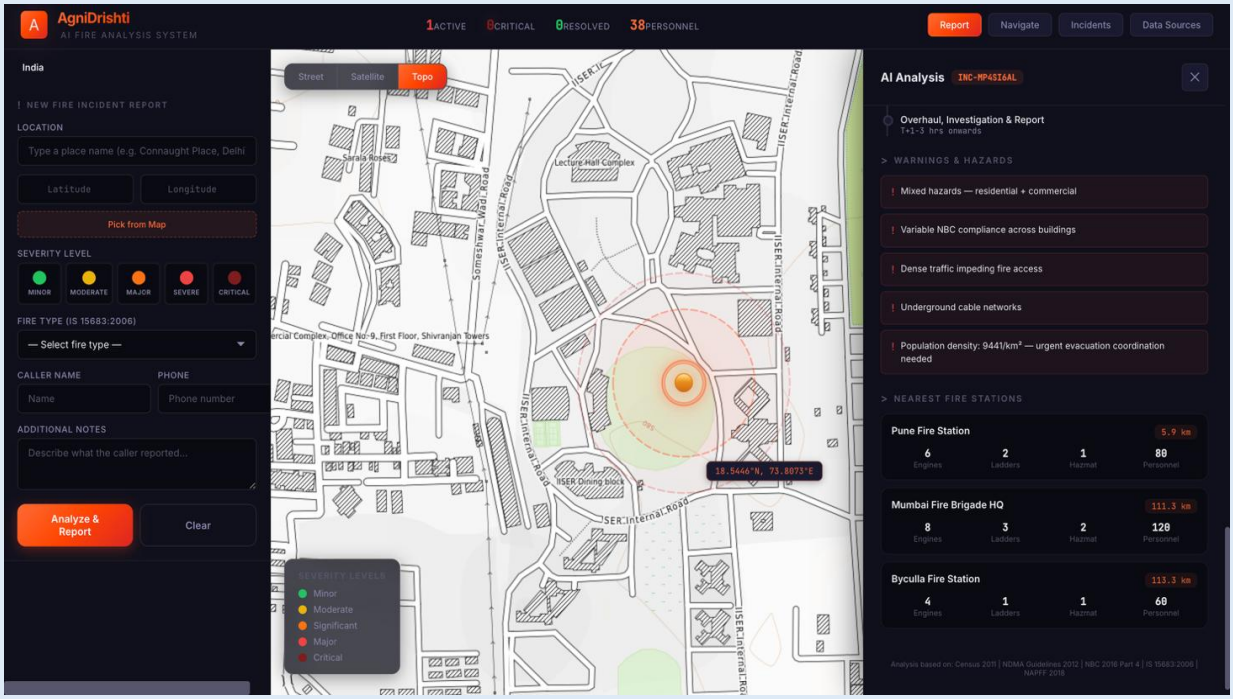

4. The location is shown on the map with 3 options – street view, satellite and topographical view.
5. AI Powered analysis is also shown adjacent.
    a. Warning hazard based on nearby topography and demography
    b. Population density
    c. Nearest fire station, hospitals etc.







6. Declaration of data source- all government data is used for analysis and classification.




7. A topographical view of the incident is shown.

## 4. AGNIDRISHTI AS DIGITAL PUBLIC INFRASTRUCTURE

DPI is characterised by three architectural properties: openness (open-source code, open standards, open data), interoperability (designed to connect with existing government systems), and scalability (deployable at national scale without per-state redevelopment). AgniDrishti satisfies all three.

Its data layer draws exclusively on nationally standardised government datasets, including Census 2011, NBC 2016, NDMA 2012, Hazardous Chemical Rules 1989, NASA FIRMS, FSI 2021 uniform across all states. The same analytical engine operates in any state fire department without redevelopment; only the incident dataset and state-specific risk parameters require localisation. Its architecture is designed for interoperability with NIC data ingestion pipelines and with state-level incident reporting systems. Its codebase has no vendor lock-in: every component is open-source and NIC-portable.

Critically, AgniDrishti converts data that fire departments already collect geo-tagged incident records, building registration logs, appliance deployment data into risk intelligence without requiring new data collection mandates or new reporting obligations. This is the defining characteristic of effective DPI: it does not create new data obligations; it creates new analytical value from existing data flows. The 40,433 geo-tagged fire incident records held by WBFES are, in AgniDrishti's architecture, not a historical archive. They are the training layer for a continuously updated risk intelligence system.

The INTOSAI Development Initiative (2023) distinguishes three levels of AI recommendation available to SAIs: Level 1 (recommend an AI strategy), Level 2 (recommend a specific AI application in a defined domain), and Level 3 (recommend a specific architecture with technical specifications). AFIRAS, as proposed here, is a Level 2 recommendation: specific enough to be actionable AI-assisted fire risk and resource allocation, NIC-hosted, fed by existing departmental data and general enough to preserve NIC's implementation autonomy and the department's operational configuration parameters.

## 5. DISCUSSION AND THE AFIRAS RECOMMENDATION

The three audit reports examined here, from West Bengal (2019), Himachal Pradesh (2022), and Tamil Nadu (2023) are not evidence of audit failure. They are evidence that the standard recommendation taxonomy has reached the practical limits of its efficacy in the fire safety domain: the recommendations are sound; their structural limitation is that they prescribe outcomes without prescribing the infrastructure capable of producing those outcomes continuously and automatically.

The DPI framework closes this gap by providing both the conceptual model and the institutional vocabulary for an infrastructure recommendation. AgniDrishti demonstrates that such a system is technically feasible, deployable on NIC infrastructure at zero licensing cost, and grounded

entirely in government-mandated data and standards. The specific recommendation proposed for consideration in the WBFES SSCA report is:

> *The Department of Fire and Emergency Services, West Bengal, may consider developing, in partnership with the National Informatics Centre, an AI-enabled Fire Risk Identification and Resource Allocation System (AFIRAS). Drawing on the Department's existing 40,433 geo-tagged fire incident records, NBC 2016-classified building data, appliance deployment logs, and seasonal risk indicators, AFIRAS would enable: continuous hazard mapping at district and station level; predictive CRI-based appliance pre-positioning; data-driven prioritisation of Fire Safety Registration inspections; early-warning generation before fire season onset; and an evidence-based investment map guiding utilisation of the 15th Finance Commission modernisation grant. AFIRAS complements, and does not replace, the manpower, infrastructure, and legislative reforms recommended separately in this report.*

INTOSAI has called on SAIs to become foresight producers (INTOSAI, 2019). The CAG has committed to AI-enabled audit operations (CAG, 2023b). AgniDrishti demonstrates that the technical barrier to extending that ambition through one carefully formulated AFIRAS recommendation in an SSCA report on fire safety has been removed by working demonstration. The question is whether it will be acted upon.

## References

Bureau of Indian Standards (BIS). (2006). IS 15683:2006 Classification of Fires. New Delhi: BIS.

Bureau of Indian Standards (BIS). (2016). National Building Code of India 2016, Part 4 Fire and Life Safety (IS SP 7:2016). New Delhi: BIS.

Central Electricity Authority (CEA). (2010). CEA (Measures Relating to Safety and Electric Supply) Regulations 2010. New Delhi: CEA.

Comptroller and Auditor General of India (CAG). (2016). Report on Urban Local Bodies, Maharashtra, Chapter IV: Results of Audit of Urban Local Bodies. New Delhi: CAG of India.

Comptroller and Auditor General of India (CAG). (2019a). Report on General and Social Sector, West Bengal, for the year ended March 2019 (Report No. 4 of 2019). New Delhi: CAG of India.

Comptroller and Auditor General of India (CAG). (2022). Report on Preparedness of the Department of Fire Services, Himachal Pradesh, Chapter IV (Report No. 3 of 2022). New Delhi: CAG of India.

Comptroller and Auditor General of India (CAG). (2023). Compliance Audit Report, Tamil Nadu, for the year ended March 2022 (Report No. 5 of 2023). New Delhi: CAG of India.

Comptroller and Auditor General of India (CAG). (2023b). Annual Report of the CAG: Technology and Audit Innovation. New Delhi: CAG of India.

Department for Promotion of Industry and Internal Trade (DPIIT). (2023). Industrial Data Zone Locations and Classifications. New Delhi: Government of India.

Forest Survey of India (FSI). (2021). India State of Forest Report 2021. Dehradun: Ministry of Environment, Forest and Climate Change.

INTOSAI. (2019). Moscow Declaration on the Role of Supreme Audit Institutions in Achieving the Sustainable Development Goals. XXIII INCOSAI, Moscow. Vienna: INTOSAI.

INTOSAI. (2023). INTOSAI Strategic Plan 2023-2028. Vienna: INTOSAI.

INTOSAI Development Initiative (IDI). (2023). Audit of Artificial Intelligence Systems in the Public Sector: A Framework for Supreme Audit Institutions. Oslo: IDI.

Ministry of Environment, Forest and Climate Change (MoEFCC). (2000). Manufacture, Storage and Import of Hazardous Chemical Rules, 1989 (amended 2000). New Delhi: MoEFCC.

Ministry of Environment, Forest and Climate Change (MoEFCC). (2018). National Action Plan on Forest Fires (NAPFF) 2018. New Delhi: MoEFCC.

NASA FIRMS. (2024). Active Fire Data MODIS/VIIRS (Terra and Aqua). NASA Earthdata. Retrieved from https://firms.modaps.eosdis.nasa.gov

National Audit Office (NAO). (2024). Use of Artificial Intelligence in Government (HC 397, Session 2023-24). London: NAO.

National Disaster Management Authority (NDMA). (2012). National Disaster Management Guidelines on Scaling, Type of Equipment and Training of Fire Services. New Delhi: NDMA.

National Informatics Centre (NIC). (2022). NIC Cloud Services Framework for State Government Applications. New Delhi: NIC-MeitY.

National Remote Sensing Centre, ISRO. (2023). Bhuvan National Geoportal. Hyderabad: ISRO.

Office of the Principal Accountant General (Audit-I), West Bengal (PAG Audit-I). (2026). Subject Specific Compliance Audit: West Bengal Fire and Emergency Services, 2023-26 Field Data and Audit Working Papers [Unpublished]. Kolkata: PAG Audit-I.

Office of the Registrar General and Census Commissioner, India. (2011). Census of India 2011: Primary Census Abstract. New Delhi: Government of India.

Standing Fire Advisory Council (SFAC). (2018). SFAC Norms for Fire Station Staffing and Equipment Standards. New Delhi: Ministry of Home Affairs.

Survey of India. (2020). State and District Boundary Data. Dehradun: Department of Science and Technology.

# Digital Public Infrastructure for Inclusive Governance: The EASE Platform for Citizen-Centric Entitlement Services in Jharkhand, India

**Bhargav Ram Khyathi**
O/o the Comptroller & Auditor General of India



## Abstract

Digital Public Infrastructure (DPI) - shared, interoperable digital systems that enable the delivery of services at societal scale (G20, 2023) - has become a central instrument of inclusive governance. While national DPIs such as India's Aadhaar and the Unified Payments Interface are well documented (IMF, 2021), less attention has been paid to how DPI design principles can be applied within the public financial management and entitlement domain at the sub-national level. This article presents the experience of the Office of the Principal Accountant General (Accounts & Entitlements), Jharkhand, India, which has built EASE (E-Administration Solution for Employees), an integrated platform that applies DPI principles - a shared identity with single sign-on, interoperable modules, open application programming interfaces (APIs) and citizen-facing service rails - to the governance of pensions, provident funds, gazetted entitlements and public grievances. The article describes the platform's architecture and its citizen- and stakeholder-facing services, including the SAMADHAN grievance-redressal system, a public pension status-tracking portal, an entitlement-tracking portal, and AI-assisted, human-in-the-loop case processing. It argues that these services advance inclusion by reducing physical visits, intermediaries and information asymmetry for pensioners, employees and citizens, while embedding auditability by design. The article concludes with observations on governance and control, the assurance role of Supreme Audit Institutions over DPI, and the replicability of a "domain DPI" model for entitlement governance across jurisdictions.

## Keywords

Digital Public Infrastructure; inclusive governance; public financial management; entitlement services; grievance redressal; Supreme Audit Institutions

## 1. Introduction

Over the past decade, Digital Public Infrastructure (DPI) has moved from a niche term to an internationally recognised driver of socio-economic development (G20, 2023). The G20 New Delhi Leaders' Declaration described DPI as an evolving concept and a set of shared digital systems, built and leveraged by both the public and private sectors, based on secure and resilient infrastructure, that can enable the delivery of services at societal scale (G20, 2023). India's own DPI - the "India Stack" comprising digital identity (Aadhaar), real-time payments (the Unified Payments Interface) and consent-based data exchange - is widely cited as a model for expanding financial inclusion and public-service delivery (IMF, 2021; World Bank, 2025).

The inclusive-governance promise of DPI rests on a small number of design principles: a shared, verifiable identity layer; interoperability through open standards and APIs; reusable building blocks rather than siloed applications; and citizen-facing rails that bring services to people rather than requiring people to travel to services (UNDP, 2023). These principles are usually discussed at a national, society-wide scale. Yet much of a citizen's actual experience of the State is mediated by sub-national and back-office institutions - treasuries, accounts offices, and pension and provident-fund authorities - whose digital maturity determines whether the promise of DPI reaches the last mile.

This article examines how one such institution - the Office of the Principal Accountant General (Accounts & Entitlements), Jharkhand, India (hereafter "the A&E Office"), a field office of the Supreme Audit Institution of India - has applied DPI design principles to the entitlement domain through an integrated platform named EASE. The objective is to document a replicable "domain DPI" and to draw out its implications for inclusive governance and the assurance role of Supreme Audit Institutions (SAIs). The discussion draws on the Office's own systems and operational records.

## 2. DPI and Inclusive Governance: A Working Frame

DPI is best understood not as a single system but as a layered set of shared rails. The widely used three-layer model comprises identity, payments and data exchange (IMF, 2021), to which a fourth, "paperless" or document layer is often added. Its inclusive-governance value arises when these layers are interoperable and reusable, allowing many services to be assembled quickly on common foundations while keeping the individual at the centre (UNDP, 2023). Inclusion, in this frame, is measured not by technical sophistication but by outcomes - whether previously excluded or underserved groups can actually access services affordably and with dignity (World Bank, 2025).

For an accounts and entitlements office, the relevant publics are pensioners (often elderly and geographically dispersed), serving employees, Drawing and Disbursing Officers (DDOs), and citizens with entitlement-related grievances. Historically, these groups depended on physical

visits, paper files and informal intermediaries to ascertain the status of a pension case, pay-fixation, a provident-fund balance or a grievance. Information asymmetry and travel costs fall hardest on the least-resourced. A domain DPI addresses this by exposing standardised, secure, self-service interfaces over a common platform.

SAIs occupy a dual position with respect to DPI: they audit it, and increasingly they build and operate it. This duality is salient for the INTOSAI community. An office that itself runs DPI must demonstrate the very controls - identity, access management, auditability and exception reporting - that it would expect to find when auditing the DPI of others. The A&E Office's platform, described below, illustrates both the opportunity and this responsibility.

## 3. The EASE Platform: A Domain DPI for Entitlement Governance

EASE (E-Administration Solution for Employees) is an integrated, web-based platform operated by the A&E Office that consolidates previously fragmented applications into a single digital workplace (Figure 1). Three design choices align it with DPI principles.

**A shared identity and single sign-on.** A common employee or office credential authenticates a user once and grants role-based access to every permitted module, removing repeated logins and parallel user databases. This mirrors the identity layer of DPI and is the foundation for interoperability.

**Interoperable, reusable modules.** Rather than standalone systems, EASE hosts modules that share data and services: The Gazetted Entitlements Management System (GEMS); pension and provident-fund modules with associated dashboards; a DAK (correspondence) management system; store, inventory and complaints modules; and the SAMADHAN grievance-redressal system. Modules exchange data through application programming interfaces (APIs) - for example, the DAK system pushes letter metadata and scanned documents into GEMS in real time, so that a case is live the moment it is received, with no manual re-entry or physical movement of paper.

**Open service rails and a common information layer.** From the EASE home screen, a Quick Links panel offers one-click entry to all modules, and a Notice Board surfaces the latest office circulars, orders and standard operating procedures with direct links, giving employees a single, authoritative place for current instructions. This functions as a lightweight data- and document-exchange layer for the institution.

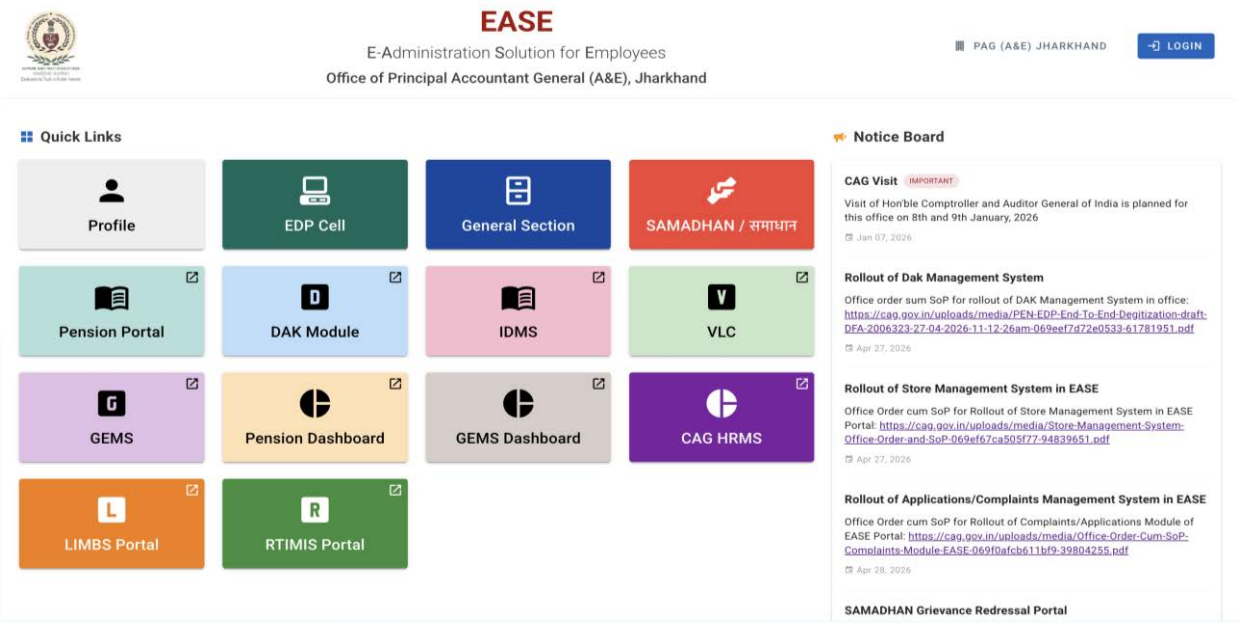



**Figure 1. The EASE platform home screen - single sign-on, a Quick Links panel to interoperable modules, and a Notice Board linking current office circulars.** ***Source: Office of the Pr. Accountant General (A&E), Jharkhand (EASE portal, 2026).***

Mapped to the DPI three-layer model, EASE provides an identity layer (shared sign-on and role-based access), a data-exchange layer (inter-module APIs and the notice/document board) and a service layer (the citizen- and stakeholder-facing portals described in Section 4). Analytics dashboards across modules provide near-real-time visibility of pendency, ageing and turnaround, and selected modules incorporate artificial-intelligence (AI) insights and forecasts under a human-in-the-loop design. In this sense EASE is a sub-national, domain-specific DPI: it does not aspire to society-wide scale, but it embodies the same architectural logic - shared identity, interoperability, reusable building blocks and open interfaces - within the entitlement-governance domain.

## 4. Enabling Inclusive Governance: Citizen- and Stakeholder-Facing Services

The inclusive-governance value of EASE is most visible in its outward-facing services, which convert internal digitisation into accessible public interfaces.

**SAMADHAN - public grievance redressal.** SAMADHAN is a citizen-facing grievance-redressal system with a public portal and an internal escalation workflow (Figure 2). A citizen or pensioner registers a grievance after one-time password (OTP) validation, receives a unique acknowledgement number and an e-receipt, and tracks status online using the reference number and mobile number; SMS alerts are triggered at registration and resolution. Internally, grievances follow a role-based escalation matrix (grievance cell → Assistant Accounts Officer → Senior Accounts Officer → disposal) with a defined turnaround target, and an AI layer categorises grievances to reveal systemic issues. By giving every grievance a reference, an owner, a visible status and a time-bound path, SAMADHAN reduces the dependence on physical visits and informal intermediaries that previously disadvantaged remote and less-resourced complainants.

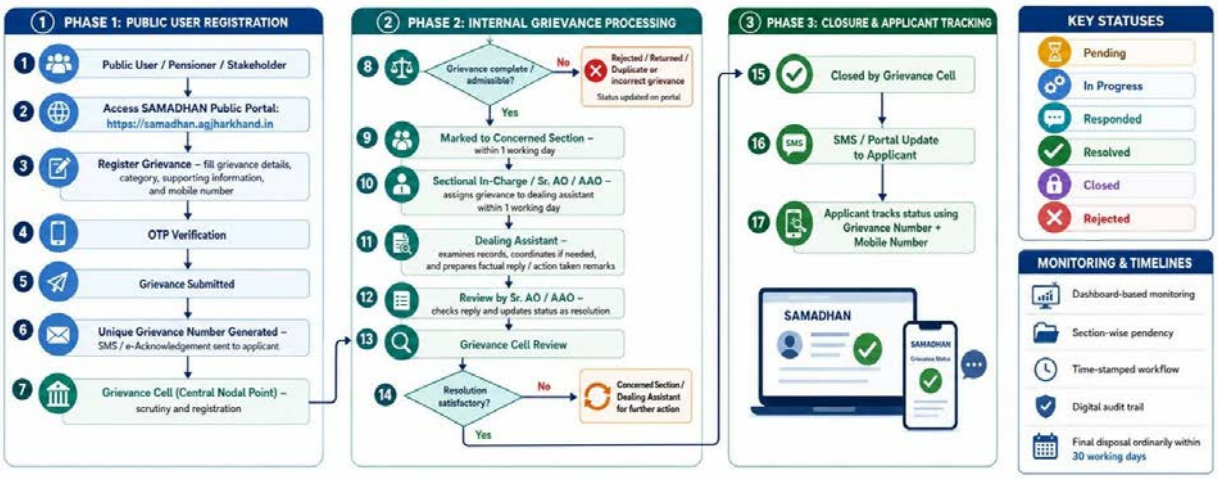



*Figure 2. The SAMADHAN public grievance-redressal portal workflow – citizens register and track grievances online after OTP validation. The Office portal provides a detailed escalation matrix for the escalation and resolution of grievances within the office. Source: Office of the Pr. Accountant General (A&E), Jharkhand (SAMADHAN portal, 2026).*

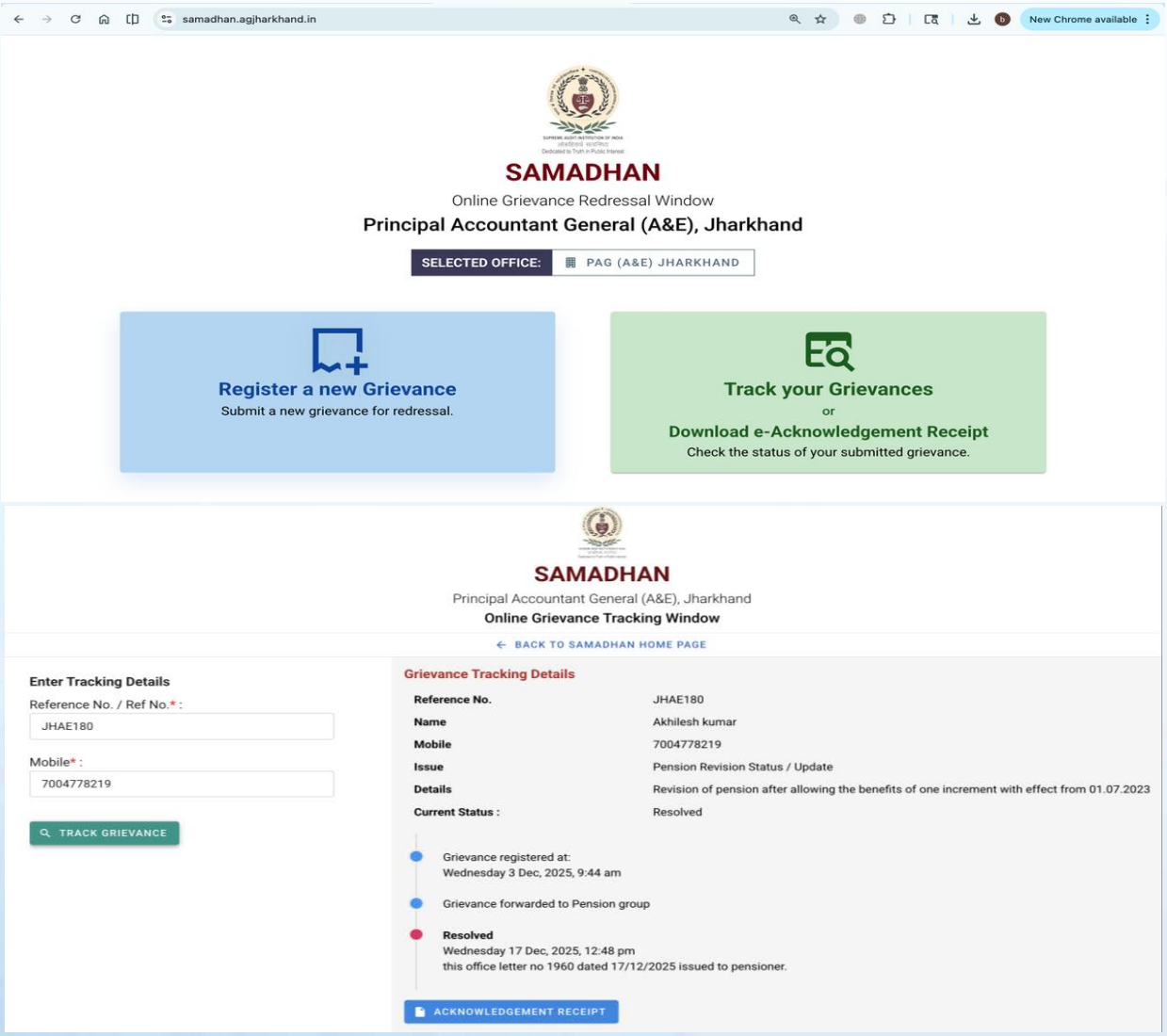
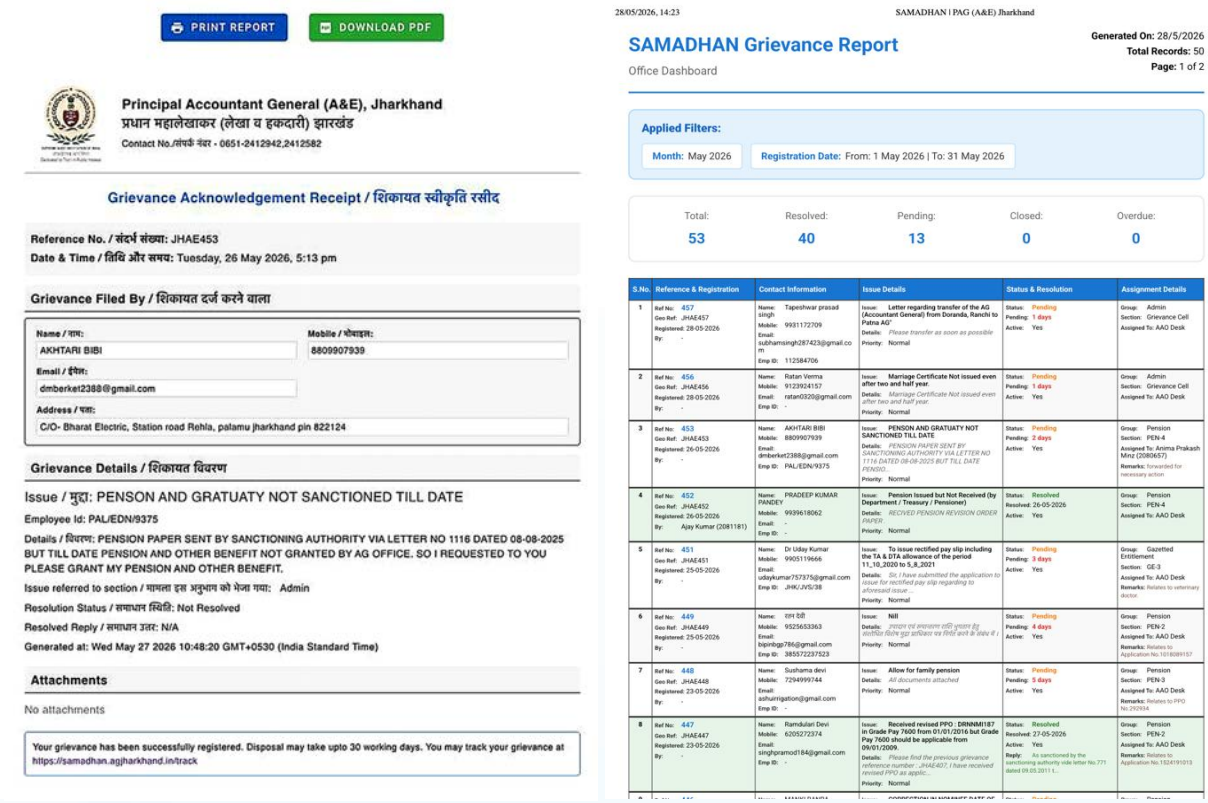



*Figure 3. The SAMADHAN public grievance-redressal portal - citizens register and track grievances online after OTP validation. Source: Office of the Pr. Accountant General (A&E), Jharkhand (SAMADHAN portal, 2026).*



PRINT REPORT DOWNLOAD PDF

Principal Accountant General (A&E), Jharkhand
प्रधान महालेखाकार (लेखा व हकदारी) झारखंड
Contact No./संपर्क नंबर - 0651-2412942,2412582

Grievance Acknowledgement Receipt / शिकायत स्वीकृति रसीद

Reference No. / संदर्भ संख्या: JHAE453
Date & Time / तिथि और समय: Tuesday, 26 May 2026, 5:13 pm

Grievance Filed By / शिकायत दर्ज करने वाला

Name / नाम: AKHTARI BIBI
Mobile / मोबाइल: 8809907939
Email / ईमेल: dmberket2388@gmail.com
Address / पता: C/O- Bharat Electric, Station road Rehla, palamu jharkhand pin 822124

Grievance Details / शिकायत विवरण

Issue / मुद्दा: PENSON AND GRATUATY NOT SANCTIONED TILL DATE
Employee Id: PAL/EDN/9375
Details / विवरण: PENSION PAPER SENT BY SANCTIONING AUTHORITY VIA LETTER NO 1116 DATED 08-08-2025 BUT TILL DATE PENSION AND OTHER BENEFIT NOT GRANTED BY AG OFFICE. SO I REQUESTED TO YOU PLEASE GRANT MY PENSION AND OTHER BENEFIT.
Issue referred to section / मामला इस अनुभाग को भेजा गया: Admin
Resolution Status / समाधान स्थिति: Not Resolved
Resolved Reply / समाधान उत्तर: N/A
Generated at: Wed May 27 2026 10:48:20 GMT+0530 (India Standard Time)

Attachments

No attachments

Your grievance has been successfully registered. Disposal may take upto 30 working days. You may track your grievance at https://samadhan.agjharkhand.in/track

28/05/2026, 14:23 SAMADHAN | PAG (A&E) Jharkhand

SAMADHAN Grievance Report

Office Dashboard

Generated On: 28/5/2026
Total Records: 50
Page: 1 of 2

Applied Filters:

Month: May 2026 Registration Date: From: 1 May 2026 | To: 31 May 2026

| Total: | Resolved: | Pending: | Closed: | Overdue: |
|---|---|---|---|---|
| 53 | 40 | 13 | 0 | 0 |

| S.No. | Reference & Registration | Contact Information | Issue Details | Status & Resolution | Assignment Details |
|---|---|---|---|---|---|
| 1 | Ref No: 457<br>Geo Ref: JHAE457<br>Registered: 28-05-2026<br>By: - | Name: Tapeshwar prasad singh<br>Mobile: 9931172709<br>Email: subhamsingh287423@gmail.com<br>Emp ID: 112584706 | Issue: Letter regarding transfer of the AG (Accountant General) from Doranda, Ranchi to Patna AG'<br>Details: Please transfer as soon as possible<br>Priority: Normal | Status: Pending<br>Pending: 1 days<br>Active: Yes | Group: Admin<br>Section: Grievance Cell<br>Assigned To: AAO Desk |
| 2 | Ref No: 456<br>Geo Ref: JHAE456<br>Registered: 28-05-2026<br>By: - | Name: Ratan Verma<br>Mobile: 9123924157<br>Email: ratan0320@gmail.com<br>Emp ID: - | Issue: Marriage Certificate Not issued even after two and half year.<br>Details: Marriage Certificate Not issued even after two and half year.<br>Priority: Normal | Status: Pending<br>Pending: 1 days<br>Active: Yes | Group: Admin<br>Section: Grievance Cell<br>Assigned To: AAO Desk |
| 3 | Ref No: 453<br>Geo Ref: JHAE453<br>Registered: 26-05-2026<br>By: - | Name: AKHTARI BIBI<br>Mobile: 8809907939<br>Email: dmberket2388@gmail.com<br>Emp ID: PAL/EDN/9375 | Issue: PENSON AND GRATUATY NOT SANCTIONED TILL DATE<br>Details: PENSION PAPER SENT BY SANCTIONING AUTHORITY VIA LETTER NO 1116 DATED 08-08-2025 BUT TILL DATE PENSIO...<br>Priority: Normal | Status: Pending<br>Pending: 2 days<br>Active: Yes | Group: Pension<br>Section: PEN-4<br>Assigned To: Anima Prakash Mnz (2080657)<br>Remarks: forwarded for necessary action |
| 4 | Ref No: 452<br>Geo Ref: JHAE452<br>Registered: 26-05-2026<br>By: Ajay Kumar (2081181) | Name: PRADEEP KUMAR PANDEY<br>Mobile: 9939618062<br>Email: -<br>Emp ID: - | Issue: Pension Issued but Not Received (by Department / Treasury / Pensioner)<br>Details: RECIVED PENSION REVISION ORDER PAPER.<br>Priority: Normal | Status: Resolved<br>Resolved: 26-05-2026<br>Active: Yes | Group: Pension<br>Section: PEN-4<br>Assigned To: AAO Desk |
| 5 | Ref No: 451<br>Geo Ref: JHAE451<br>Registered: 25-05-2026<br>By: - | Name: Dr Uday Kumar<br>Mobile: 9905119666<br>Email: udaykumar757375@gmail.com<br>Emp ID: JHK/JVS/38 | Issue: To issue rectified pay slip including the TA & DTA allowance of the period 11_10_2020 to 5_8_2021<br>Details: Sir, I have submitted the application to issue for rectified pay slip regarding to aforesaid issue...<br>Priority: Normal | Status: Pending<br>Pending: 3 days<br>Active: Yes | Group: Gazetted Entitlement<br>Section: GE-3<br>Assigned To: AAO Desk<br>Remarks: Relates to veterinary doctor. |
| 6 | Ref No: 449<br>Geo Ref: JHAE449<br>Registered: 25-05-2026<br>By: - | Name: राम देवी<br>Mobile: 9525653363<br>Email: bajinbgr786@gmail.com<br>Emp ID: 385572237523 | Issue: Nill<br>Details: ...उपरोक्त एवं सम्बन्धित तहसील मुख्यालय हेतु आवेदिका विधवा सुख सम्बियता पर विचार करने के संबंध में ।<br>Priority: Normal | Status: Pending<br>Pending: 4 days<br>Active: Yes | Group: Pension<br>Section: PEN-2<br>Assigned To: AAO Desk<br>Remarks: Relates to Application No.1018089157 |
| 7 | Ref No: 448<br>Geo Ref: JHAE448<br>Registered: 23-05-2026<br>By: - | Name: Sushama devi<br>Mobile: 7294999744<br>Email: ssihurirrigation@gmail.com<br>Emp ID: - | Issue: Allow for family pension<br>Details: All documents attached<br>Priority: Normal | Status: Pending<br>Pending: 5 days<br>Active: Yes | Group: Pension<br>Section: PEN-3<br>Assigned To: AAO Desk<br>Remarks: Relates to PPO No.292934 |
| 8 | Ref No: 447<br>Geo Ref: JHAE447<br>Registered: 23-05-2026<br>By: - | Name: Ramdulari Devi<br>Mobile: 6205272374<br>Email: singhpramod184@gmail.com<br>Emp ID: - | Issue: Received revised PPO : DRNNM1187 in Grade Pay 7600 from 01/01/2016 but Grade Pay 7600 should be applicable from 09/01/2009.<br>Details: Please find the previous grievance reference number: ...JHAE407, I have received revised PPO as applic...<br>Priority: Normal | Status: Resolved<br>Resolved: 27-05-2026<br>Active: Yes<br>Reply: As sanctioned by the sanctioning authority vide letter No.771 dated 09.05.2011 t... | Group: Pension<br>Section: PEN-2<br>Assigned To: AAO Desk<br>Remarks: Relates to Application No.1524191013 |

***Figure 4 and 5. Illustrative grievance e-acknowledgement receipt generated by the portal for future reference and tracking by the grievant, SAMADHAN dashboard-generated grievance report showing filtered monthly grievance status, including total, resolved, pending, closed and overdue cases with case-wise tracking details***

**Pension and entitlement Self-Service Portals.** A public-facing pension status-tracking portal allows pensioners, DDOs and other stakeholders to track a live pension case by reference number, GPF details or DDO-wise status, and to view and download current and previous documents from a secure archive. A companion Gazetted Entitlement Tracking Portal lets gazetted officers authenticate by entitlement number and registered mobile number (OTP) and check the status of pay-slips, pay-fixation and other entitlement applications. These self-service rails are particularly consequential for elderly pensioners and for officers posted away from the State capital, for whom a physical visit to ascertain case status is costly and sometimes infeasible.

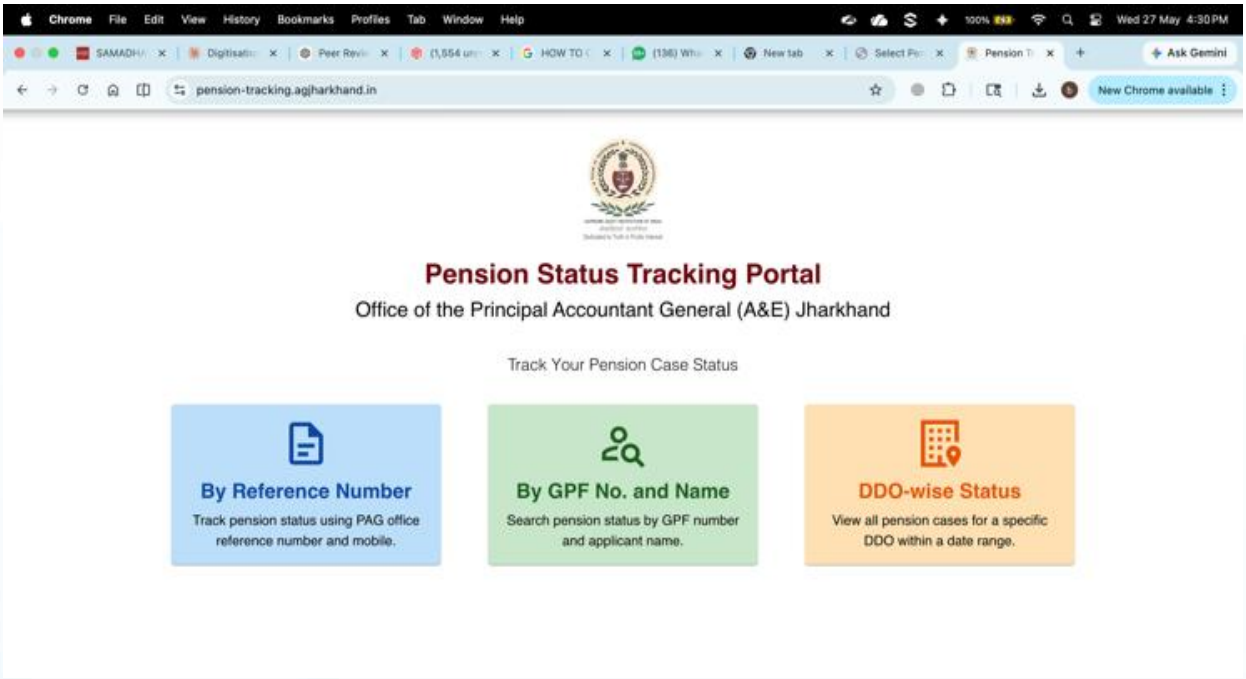



*Figure 6. Public-facing Pension Status Tracking Portal enabling pensioners, DDOs and stakeholders to track live pension cases through reference number, GPF details or DDO-wise status.*

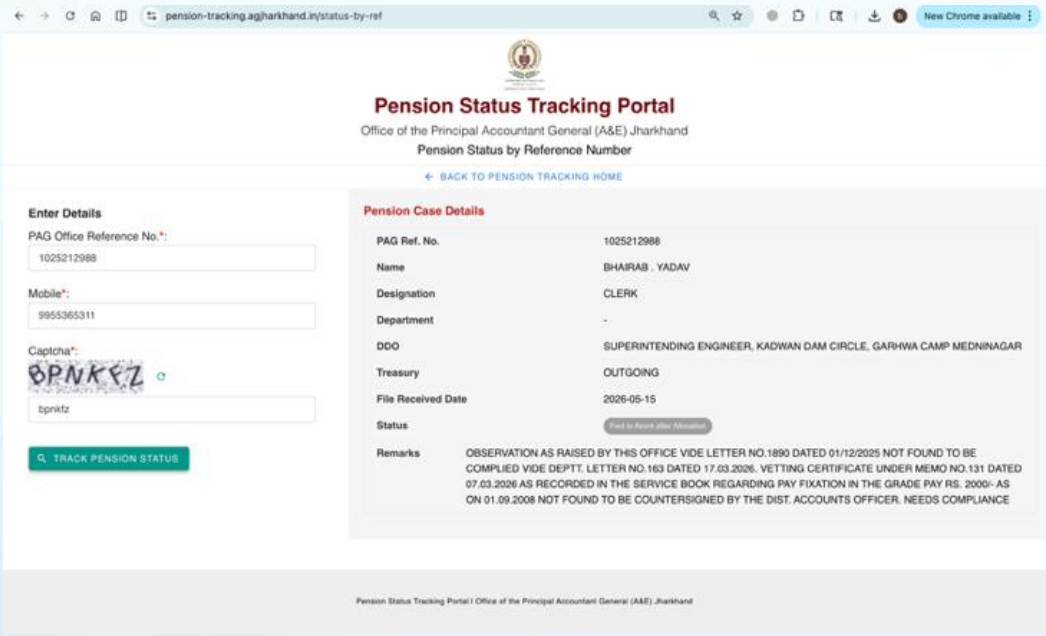



*Figure 7. Case status output displaying PAG reference number, employee details, DDO, treasury, file received date, present status and office remarks/action required*

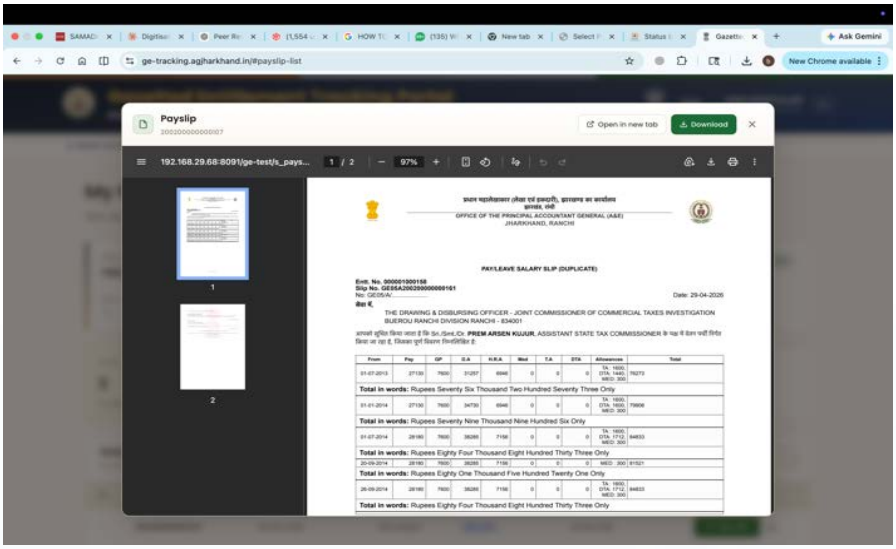



*Figure 8. Current/Previous Payslips viewing functionality for gazetted officers on real time basis*

**Transparency and assurance by design.** Across modules, role-based dashboards expose total, pending, resolved and returned cases, pendency ageing and average processing time at section and seat level (Figure 9, 10 and 11). This transparency serves two audiences at once: supervisory officers, who can monitor turnaround times and identify bottlenecks; and, through the citizen portals, the public, who can see that a case is progressing. AI-assisted features - for example, optical-character-recognition-based pre-screening of correspondence and forecasting of case volumes - are deployed as decision support, with the human officer retaining the final decision. This human-in-the-loop posture is a deliberate inclusion and accountability safeguard: it keeps a responsible officer answerable for every outcome while using automation to reduce delay and error.

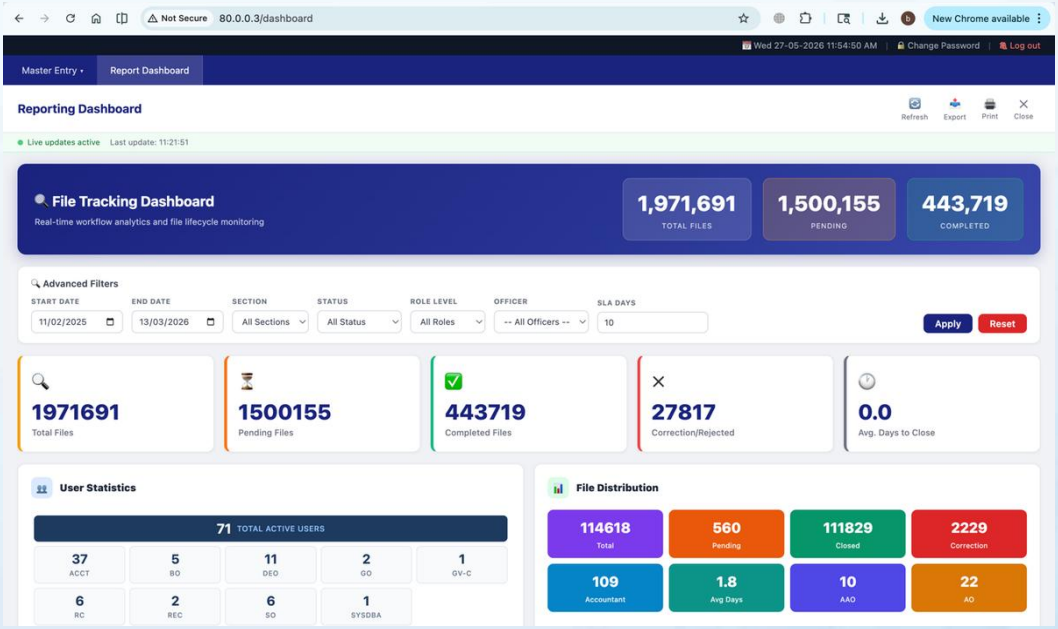



*Figure 9. Pension monitoring dashboard in office - near-real-time visibility of total, pending and completed cases, pendency ageing and turnaround. Source: Office of the Pr. Accountant General (A&E), Jharkhand (EASE dashboards, 2026).*

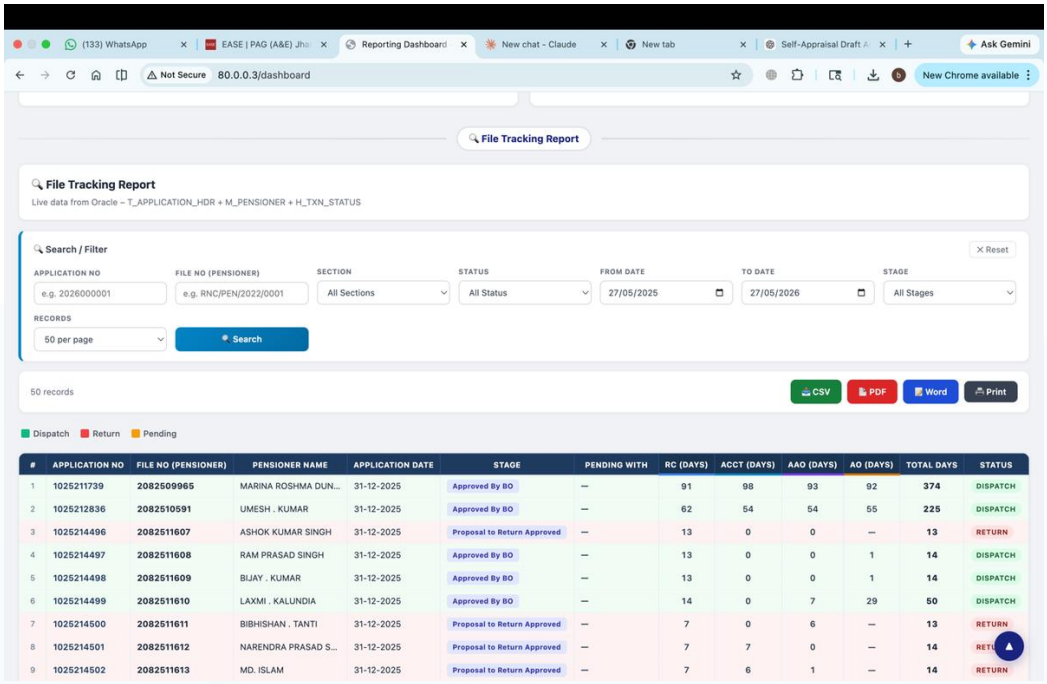



*Figure 10: File Tracking Report with red flags for cases exceeding the 30 day threshold*

## GEMS (Gazetted Entitlement Management System) Reporting Dashboard

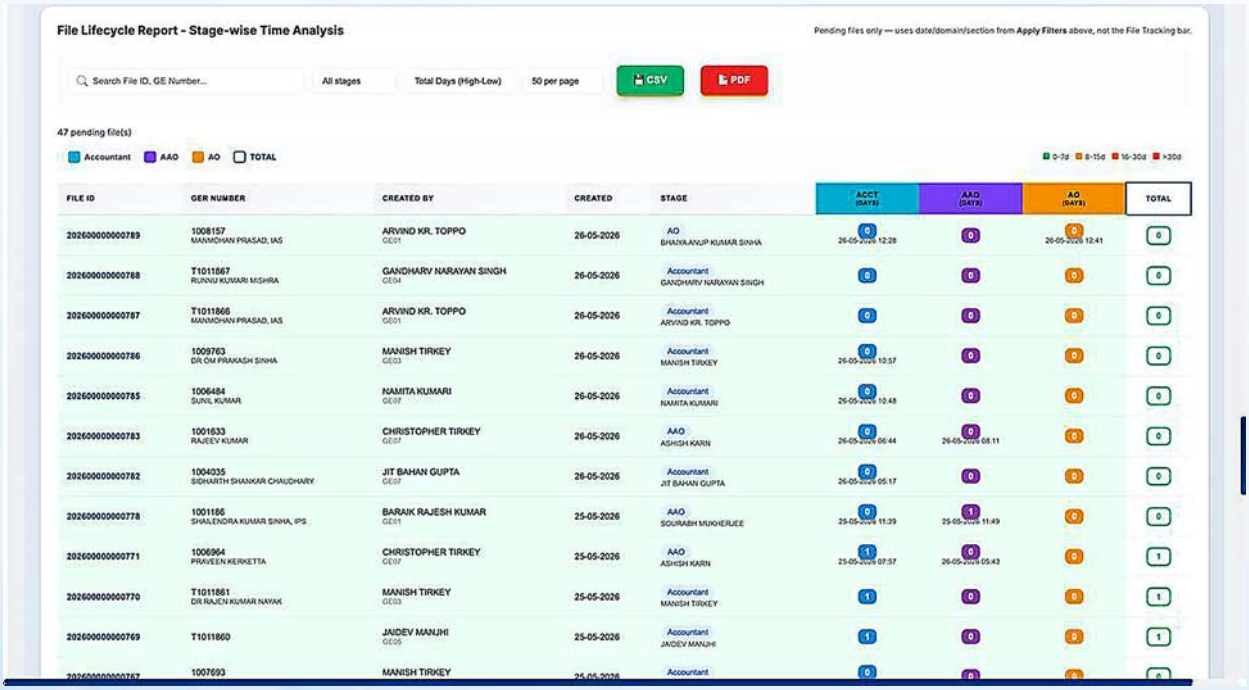



*Figure 11: File Lifecycle Report - stage-wise ageing and time analysis of pending cases*

Taken together, these services illustrate the inclusion mechanism of a domain DPI: standardised, secure, self-service access reduces travel, cost, intermediation and information asymmetry, and shifts the burden of coming to the office from the citizen to the system.

## 5. Governance, Controls and the Audit Dimension

A platform that consolidates identity, data and services also concentrates risk, and a Supreme Audit Institution operating such a platform must hold itself to the same standards it applies to others. EASE embeds several controls consistent with good DPI governance: a single identity with role-based access; audit trails and case histories that make actions traceable; and dashboards and exception views that function as continuous, near-real-time monitoring rather than periodic, sample-based review. These features make the platform auditable by design.

The dual role of SAIs over DPI deserves emphasis for the INTOSAI community. As public services migrate onto shared digital rails, assurance must extend beyond financial regularity to the integrity of the rails themselves - identity and access management, maker-checker controls over master data, application-level validation, logging and exception reporting. Experience across jurisdictions shows that weak controls in shared financial systems can enable large-scale irregularities; conversely, the same data that flows through a DPI can be harnessed for continuous, analytics-led assurance. An office that has built its own domain DPI is well placed to understand both the control requirements and the analytical opportunities, and to carry that understanding into its audit of other digital systems.

## 6. Discussion and Conclusion

The EASE experience suggests three observations of wider relevance. First, the architectural logic of DPI - shared identity, interoperability, reusable building blocks and open interfaces - is scale-independent: it can be applied productively within a single institution and a single domain, not only at national scale. Second, the inclusive-governance dividend of such a domain DPI is concrete: fewer physical visits, faster and more transparent service, and reduced reliance on intermediaries for pensioners, employees and citizens. Third, when the institution operating the platform is a Supreme Audit Institution, building DPI and assuring DPI become mutually reinforcing capabilities.

Several implications follow. For practitioners, the priority is not bespoke applications but common rails - identity, APIs and shared data - on which many services can be assembled and reused. For inclusion, citizen-facing self-service must be designed for the least-resourced user, through OTP-based access by mobile number, online status tracking, downloadable documents and SMS touchpoints. For governance, auditability should be designed in from the outset through identity, access control, master-data controls and exception reporting. For SAIs specifically, operating a domain DPI is an opportunity to model the controls they expect elsewhere and to build the data-analytics capacity that modern, DPI-mediated public finance increasingly demands.

In conclusion, Digital Public Infrastructure is not only a national project; its principles can be embedded in the everyday machinery of entitlement governance to make that machinery more

inclusive, transparent and accountable. The A&E Office's EASE platform offers one replicable template - a sub-national, domain-specific DPI - for institutions seeking to bring the promise of inclusive digital governance closer to the citizens they serve.

## References


G20. (2023). *G20 New Delhi Leaders' Declaration*. Group of Twenty.

International Monetary Fund. (2021). The India Stack is revolutionizing access to finance. *Finance & Development*. International Monetary Fund.

United Nations Development Programme. (2023). *The DPI approach: A playbook*. UNDP.

World Bank. (2025). *Digital public infrastructure: Setting standards with the hourglass model*. World Bank.

Office of the Principal Accountant General (A&E), Jharkhand. (2026). *EASE: E-Administration Solution for Employees - System documentation and operational records*

# Who Benefits from Digital Public Infrastructure? Auditing Inclusion, Accountability, and Service Delivery Outcomes

**Maha Fathy Ibrahim Morsy**
Accountability State Authority, Egypt



## Introduction

Digital Public Infrastructure (DPI) has become one of the fundamental pillars of digital transformation efforts worldwide. Governments are increasingly investing in digital identity systems, digital payment platforms, interoperable data exchange mechanisms, and integrated service portals to improve public service delivery and strengthen inclusive governance.

The Organisation for Economic Co-operation and Development (OECD) defines Digital Public Infrastructure (DPI) as a set of shared, secure, and interoperable digital systems that support broad access to public and private services across society. These systems constitute the foundational building blocks upon which governments develop and deliver digital services efficiently, consistently, and at scale. The growing adoption of Digital Public Infrastructure has been accompanied by high expectations of improved public services, increasing efficiency, enhancing transparency, and achieving greater inclusion.

Nevertheless, despite the substantial investments directed toward this area, one fundamental question remains:

## Who actually benefits from Digital Public Infrastructure?

This question is particularly significant considering what **INTOSAI-P 12** emphasizes: that Supreme Audit Institutions should make a difference to the lives of citizens by promoting accountability, transparency, and good governance. This makes the assessment of outcomes and the impact achieved for citizens an essential component of the audit process.

Accordingly, the success of Digital Public Infrastructure should not be measured solely by the number of platforms launched, the volume of transactions processed, or the number of registered users. Rather, it should be assessed by its ability to deliver tangible outcomes for citizens, particularly the most vulnerable and underserved groups, while ensuring accountability,

transparency, and the efficient use of public resources. As governments continue to expand digital systems and services, the role of Supreme Audit Institutions becomes increasingly important in determining whether Digital Public Infrastructure initiatives are achieving their intended objectives and generating real value for society.

## From Digital Infrastructure to Public Outcomes

Most international discussions on Digital Public Infrastructure (DPI) focus on its technical capabilities and potential advantages, such as improving efficiency, enhancing interoperability, increasing resilience and scalability, and improving user experience. However, these advantages do not necessarily guarantee better public outcomes. A digital infrastructure may fail to reach its intended beneficiaries, continue to suffer from poor data quality, or result in the exclusion of groups that are less able to use or access digital technologies.

Therefore, auditors should go beyond assessing the technical aspects of implementation and focus on the extent to which Digital Public Infrastructure contributes to achieving tangible outcomes for citizens. This includes assessing whether eligible citizens are actually receiving the intended services, whether access to those services has become easier, whether administrative burdens have been reduced, and whether real value has been achieved from the use of public resources. Accordingly, Digital Public Infrastructure becomes an issue of governance, accountability, and public impact, requiring a shift from measuring outputs to evaluating outcomes.

## Auditing Methodology for Digital Public Infrastructure

### Why Does Auditing Digital Public Infrastructure Require a Different Approach?

This shift in the assessment perspective requires the adoption of an audit methodology that goes beyond the scope of traditional information technology audits. While such audits often focus on internal controls, cybersecurity, infrastructure management, and compliance with regulatory requirements, auditing Digital Public Infrastructure also requires assessing the extent to which it contributes to achieving government objectives and improving public service delivery. This is because Digital Public Infrastructure operates at the intersection of technology, governance, public service delivery, and social inclusion. Therefore, auditors need to integrate multiple tools and approaches, including information technology auditing, performance auditing, and governance assessment, supported by risk analysis and data analysis. This integrated approach enables auditors to develop a comprehensive understanding of performance and outcomes.

The audit process begins with understanding the digital system under examination and mapping the flows of data, decisions, and services among participating entities, thereby helping to identify key processes, interrelationships, and potential areas of weakness. Data analysis is one of the most important audit tools in this field. By analysing beneficiary data, transaction data,

eligibility criteria, and service usage patterns, auditors can identify duplicate transactions, unusual transactions, and risks of exclusion.

Auditors can also identify indicators of inefficiency or misuse. Examples of indicators that can be analysed include the percentage of applications rejected due to data errors, the rate of completion of digital transactions, the number of unsuccessful identity verification attempts, and variations in service utilization rates across geographical regions or different population groups.

Since Digital Public Infrastructure relies on data exchange among different institutions, data quality and interoperability should also be assessed, with particular emphasis on data accuracy, completeness, consistency, and timely updating. In parallel, governance arrangements and internal control mechanisms should be evaluated, including user access management, cybersecurity controls, change management procedures, and business continuity plans. This integrated approach contributes to providing a comprehensive assessment of the efficiency and effectiveness of Digital Public Infrastructure. Accordingly, the assessment of performance is not limited to the efficiency of the technology employed, but also extends to the extent to which it contributes to achieving public objectives, improving public services, and enhancing public value for citizens.

In applying this methodology to achieve the objective of this article, the audit procedures were based on the Egyptian Auditing Standards and guided by the INTOSAI standards, including ISSAI 100, ISSAI 300, and ISSAI 400, together with their corresponding guidance documents, as well as the relevant publications of the Accountability State Authority. In addition, the COBIT framework was used to assess information technology governance and controls during the audit of a digital system designed to support access to medicines for the most vulnerable groups.

## Case Study: Auditing the State-Funded Medical Treatment System for Low-Income Citizens

Medicine support programmes aim to ensure that low-income citizens and patients with chronic diseases have access to essential medicines without the cost becoming a financial burden that prevents them from obtaining the necessary healthcare. To achieve this objective, the Egyptian government developed an integrated digital system that connects digital identity databases, health insurance records, medical records, social insurance databases, contracted pharmacies, and electronic payment systems, with the aim of ensuring that support is directed to eligible beneficiaries and improving the efficiency of programme administration.

### Audit Objective

The audit aimed to assess the effectiveness of the digital system in ensuring that pharmaceutical support reaches eligible beneficiaries, evaluate the efficiency and transparency of the service

delivery process, and verify the adequacy of internal controls and the protection of data used in managing the programme.

## Audit Scope

The audit covered the entire service delivery cycle, starting from beneficiary registration, eligibility verification, and prescription issuance, through the dispensing of medicines by participating pharmacies, and ending with payment settlement and charging the cost of the subsidy to the relevant government entities. The audit also included an assessment of data exchange among participating entities and the reliability of the data used in determining eligibility and providing pharmaceutical support.

## Audit Methodology Applied

The audit team adopted a combination of information technology auditing, performance auditing, and data analysis techniques. Within this framework, the following procedures were performed:

- Mapping the flow of data among participating entities.
- Reviewing internal controls over user management and access rights.
- Assessing cybersecurity and medical data protection measures.
- Testing the quality of the data used to identify eligible beneficiaries.
- Analysing beneficiary and transaction data using data analytics tools.

## Data Analytics Tests

Data analytics techniques were used to identify potential risk indicators, including:

- Identifying duplicate beneficiaries using the national identification number or personal data.
- Detecting multiple dispensations of the same prescription.
- Analysing unusually high-cost medicine dispensations.
- Comparing social eligibility data with the records of actual beneficiaries.

## Key Challenges

### 1. Data Quality and Integration

Eligibility decisions and service delivery rely on data obtained from multiple entities, increasing the risk of incomplete, inconsistent, or outdated data.

**2. Interoperability Across Different Systems**

Limited integration among participating databases and systems may hinder the accurate and timely exchange of information, thereby affecting the efficiency of service delivery.

**3. Ensuring Service Delivery to Target Beneficiaries**

Verifying that services reach eligible beneficiaries across different geographical areas and social groups represents one of the most significant audit challenges, particularly in light of disparities in digital literacy and access to digital services.

**4. Data Protection and Cybersecurity**

The system processes large volumes of sensitive health and personal data, creating challenges related to data confidentiality and protection against unauthorized access or misuse.

## Main Audit Results

The audit found that the digital system made a significant contribution to improving the efficiency of delivering subsidized medicines, by accelerating service delivery procedures, reducing reliance on paper-based processes, enhancing the accuracy of beneficiary eligibility verification, strengthening transaction traceability, and providing data to support informed decision-making. The system also contributed to improving transparency, standardizing service delivery procedures, and enhancing the beneficiary experience by reducing the time required to obtain the service.

The audit further found that the adoption of digital databases and their integration with multiple government entities represents an important step towards strengthening the efficiency of the subsidy scheme and improving the targeting of eligible beneficiaries, thereby supporting the optimal use of public resources and reinforcing the role of digital public infrastructure in delivering more efficient and inclusive public services.

The audit also identified opportunities to further maximize the benefits achieved through the digital system and enhance their sustainability. These include the continued enhancement of mechanisms for the timely updating of databases used to verify eligibility, thereby improving the accuracy of beneficiary targeting and ensuring that support continues to reach those who are entitled to it; expanding the use of data analytics to identify unusual transaction patterns, thereby strengthening preventive oversight; and further enhancing controls over privileged user accounts and continuous monitoring mechanisms, thereby supporting system security, preserving data integrity, and ensuring the continued delivery of services in an efficient and reliable manner.

## Conclusion

By integrating information technology auditing, performance auditing, governance assessment, and risk and data analysis, auditors can develop a comprehensive understanding of the performance and outcomes of Digital Public Infrastructure. This approach enables the assessment of the technical aspects of digital systems while also evaluating the extent to which they contribute to improving access to public services, enhancing efficiency and accountability, and ensuring that public benefits reach their intended beneficiaries. As a result, the audit process becomes more comprehensive, combining the assessment of the efficiency of the technical system with the evaluation of its actual impact on citizens.

## References


Desai, A., & Manoharan, A. P. (2024). Digital transformation and public administration: The impacts of India's digital public infrastructure. *International Journal of Public Administration*. https://doi.org/10.1080/01900692.2024.2348456

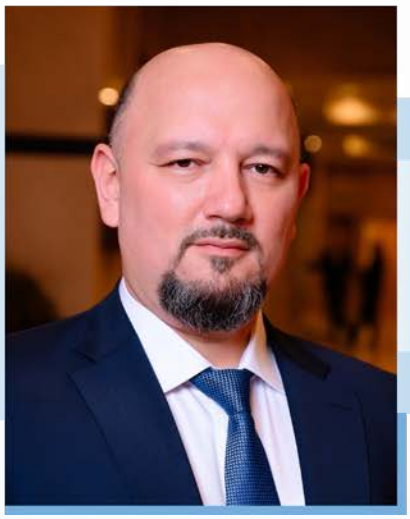
Djatmiko, G. H., Sinaga, O., & Pawirosumarto, S. (2025). Digital transformation and social inclusion in public services: A qualitative analysis of e-government adoption for marginalized communities in sustainable governance. *Journal of Multidisciplinary Research*.

Sain, Z., Aziz, A. L., Lawal, U. S., Abdullah, N., & Sain, S. H. (2025). Evaluating the impact of digital transformation on public service delivery efficiency and accountability. *Journal of Multidisciplinary Research*.

OECD. (2024). *Digital public infrastructure for digital governments*. OECD Public Governance Policy Papers No. 68. OECD Publishing. https://doi.org/10.1787/3f6a0e6a-en

# From AI Access to Ethical Readiness: Auditing AI-Enabled Education DPI for Inclusive Governance

*Reflections from India Stack and Uzbekistan's Emerging Experience*



**Rustamkhuja Ishanov**

Head of Department, UZINFOCOM LLC under Ministry of Digital Technologies, Republic of Uzbekistan

## Abstract

Digital Public Infrastructure (DPI) is becoming a foundation of inclusive governance. Most discussions still centre on identity, payments, data exchange and service delivery. Yet the next stage of DPI will be shaped by artificial intelligence, and education is where the shift will be felt most directly. AI-enabled education platforms can support teachers, personalise learning and widen access to quality content. They also raise moral and governance questions that technical controls alone cannot answer. Drawing on lessons from India Stack, the DPI Safeguards discussions at the 166th International Training Programme on Audit of DPI at the International Centre for Information Systems & Audit (iCISA), and the author's own involvement in Uzbekistan's AI-based teacher assistant initiative and in work connected with UNESCO's AI Readiness Assessment Methodology, this article makes a simple argument: an AI education system can be technically ready and still be ethically unprepared. Inclusive governance in education has to protect critical thinking, academic honesty, child data privacy, teacher agency and moral-ethical development. To make that protection auditable, the article proposes an ethical-readiness lens for AI-enabled education DPI — a set of questions that help auditors and policymakers judge whether a system supports human development or simply automates content delivery.

## Keywords

Digital Public Infrastructure; Artificial Intelligence; Education; Ethical Readiness; Inclusive Governance; DPI Audit

## 1. Introduction

Digital Public Infrastructure (DPI) has become one of the central ideas in modern public governance. India Stack is one of the most prominent examples: digital identity, interoperable

payments, consent-based data exchange and sectoral platforms, combined into a foundation for service delivery at population scale. It is officially described as a set of open APIs and digital public goods built to unlock identity, data and payments at that scale (India Stack, n.d.).

The 166th International Training Programme on Audit of DPI at the International Centre for Information Systems and Audit (iCISA) was an opportunity to study DPI not as a set of applications but as public infrastructure. The lesson that stayed with me was simple: DPI only becomes meaningful when it is inclusive, interoperable, auditable and trusted. This became especially clear during the discussion of ASOSAI cases. The presentation on Thailand's ageing society showed how DPI access can become difficult for vulnerable groups if awareness, support and coordination are weak. The Indonesian case, with its focus on the digital divide, privacy and interoperability, made the same point from another angle. For me, that session turned the word "inclusive" from an abstract principle into an audit question: who may be left behind, and how do we know it?

The future of DPI, though, will not be decided by identity and payment systems alone. Artificial intelligence is now entering public services, including education. In schools it can help teachers, recommend materials, track performance and close learning gaps. It can also produce answers that are wrong but convincing, erode critical thinking, make cheating easier, and widen the gap between learners with good tools and those without.

This article asks one question. How should AI-enabled education DPI be governed and audited so that it supports inclusive governance without weakening the moral and intellectual foundations of education?

## 2. DPI, Inclusion and the Role of Audit

DPI is often compared to roads, railways or electricity grids. It is not a single application but a set of reusable digital building blocks that let public and private services operate at scale. In India these include Aadhaar, the Unified Payments Interface, DigiLocker, eSign, the Goods and Services Tax Network, the Ayushman Bharat Digital Mission and digital education platforms.

The real strength of the model is architectural, not just technological. DPI works when systems share common standards, open interfaces, clear governance and safeguards. When every ministry builds its own isolated system, transformation stays fragmented. When the core rails are shared, services scale faster and reach further.

Inclusive governance through DPI therefore demands more than putting services online. Citizens have to be able to reach those services; data has to be handled responsibly; vulnerable groups must not be designed out; and public institutions need to be able to audit how the systems actually work. Seen this way, audit is not an external formality bolted on at the end. It is part of the trust infrastructure.

The Universal DPI Safeguards Framework makes the same point: digital public infrastructure should mitigate risks, advance trust and equity, and protect individuals and societies across the whole DPI lifecycle (UNDP & OSET, 2024). That logic matters even more once artificial intelligence is embedded into education.

## 3. AI in Education: Opportunity, Risk and Ethical Readiness

Artificial intelligence adds a new layer to DPI. In education, AI can analyse student progress, flag weak areas, recommend materials and support personalised learning. For countries with uneven teacher capacity or wide regional gaps, that can be real value, not just novelty.

Uzbekistan has started down this road. The national Strategy for the Development of Artificial Intelligence Technologies until 2030 was approved by Presidential Resolution No. PQ-358 of 14 October 2024, with the aim of expanding AI use across the social and economic sectors (President of the Republic of Uzbekistan, 2024). Cabinet of Ministers Resolution No. 425 of 10 July 2025 then approved a list of priority AI projects for 2025-2026 (Cabinet of Ministers of the Republic of Uzbekistan, 2025). One of them is an AI-based teacher assistant, “Pedagog yordamchi”, meant to analyse how well students have mastered subjects and recommend material to close the gaps.

I have been involved in the conceptual work on this teacher assistant, and from the start I argued for building AI ethics into the design rather than adding it later. One practical design decision was particularly important: the platform should not become a generator of ready-made answers for students or an autopilot for teachers. Its safer role is to work as a recommendation and decision-support layer: to analyse mastery gaps, suggest relevant learning materials and leave the final pedagogical decision with the teacher. This shift from generation to guided recommendation is an ethical safeguard, not merely a technical choice. It reduces the risk of academic dishonesty, protects teacher agency and responds to emerging regulatory concerns around accountability and child data protection. That experience is what convinced me of the main point of this article: an education AI system has to be judged on ethical readiness, not only technical readiness.

The same conclusion comes out of work related to UNESCO’s AI Readiness Assessment Methodology. Ethical readiness is not a decorative add-on to AI governance; it is a precondition for responsible adoption, and especially so in a sector as sensitive as education. UNESCO describes the methodology as a tool that helps Member States find the institutional and regulatory gaps in implementing the Recommendation on the Ethics of Artificial Intelligence (UNESCO, n.d.).

The real risk in education is not the abstract fear that AI will “replace thinking”. It is more concrete. AI can write essays, tests, summaries, analyses, even administrative documents. If a student or a teacher cannot critically check what comes back, they start treating generated text

as fact. AI writes fluently, but fluency is not correctness: its reasoning can be hollow because it lacks context, local knowledge or any moral judgement.

In a classroom that is dangerous. A teacher who cannot evaluate AI-generated material may pass weak reasoning straight on to students. A student who submits AI-generated work as their own may not even register that this is dishonesty rather than "just using technology". So AI in education is never only a technical question. It is a moral and educational one.

## 4. Moral-Ethical Education Before AI Use

In Uzbek intellectual and educational tradition, the idea of *ma'naviy-axloqiy tarbiya* — moral and ethical upbringing — sits at the centre of how a person is formed. With AI in the picture, it matters more, not less.

AI is not the foundation of education. It is an instrument laid on top of a moral and intellectual foundation that has to exist first. If a learner has not yet developed honesty, responsibility, respect for others and a sense of consequences, AI stops being a tool for learning and becomes a tool for avoiding it.

Take the obvious case. A student writes a prompt, gets a finished answer, and hands it in as their own. Technically, they used an advanced tool. Ethically, they dodged the work. If the system never draws that line for them, AI quietly normalises dishonesty.

This is why moral-ethical education has to come before AI adoption, not after; UNESCO's guidance on generative AI in education makes the same case for policies, safeguards and human capacity ahead of deployment (UNESCO, 2023). Students need to learn that AI output must be checked; that using it without saying so can be dishonest; that the human user, not the model, owns the final answer; that no tool replaces personal judgement; and that knowledge is understanding, not just information.

Parents and teachers share this work. Parents lay the first moral foundation; teachers turn it into study habits, academic honesty and critical thinking. AI should reinforce that relationship, not quietly hollow it out.

## 5. The Role of the Teacher in an AI-Enabled Education DPI

A common worry is that AI will replace teachers. I do not think it will, and I do not think it should. A teacher does far more than transmit information — they motivate, guide, read the room, notice when a student is struggling, and help shape character over time.

The more realistic danger is quieter: the teacher becomes a passive operator of the tools. If the platform generates the lesson plans, the assessments, the feedback and the recommendations, and the teacher simply accepts them, the profession loses the very part that makes it formative.

The design principle that prevents this is **teacher-in-the-loop**. The teacher stays the final pedagogical authority; AI may analyse, recommend and support, but interpretation, adaptation and responsibility remain human. UNESCO's Recommendation on the Ethics of Artificial Intelligence makes the same demand — human oversight, transparency, accountability and the protection of human dignity (UNESCO, 2021).

This is also an audit concern, not only a pedagogical one, and Section 7 turns it into concrete questions.

## 6. Inequality and the New Digital Divide

AI in education can narrow inequality or widen it, depending on how it is rolled out. Some teachers and students already work with advanced AI; others still do not have a stable internet connection. Left unmanaged, that produces two cohorts of learners — one amplified by powerful tools, one left outside them.

So inclusion cannot be measured by whether a platform exists. It has to be measured by whether every school, teacher and student can actually use it: access to the internet and devices, teacher training, content in the local language, child-protection standards, transparency about how recommendations are produced, a way to appeal or correct them, and protection of personal data.

Without those, AI-enabled education DPI tends to reach the already-advantaged first and the rest much later, if at all. Meaningful access, not formal availability, is what inclusive governance has to deliver.

## 7. An Ethical-Readiness Lens for AI-Enabled Education DPI

Lessons from iCISA, India Stack, the DPI Safeguards work and AI readiness assessment all point in the same direction: AI-enabled education DPI should be audited for more than efficiency, cybersecurity and uptime. It should be audited for ethical readiness. The lens below is a starting set of questions for auditors and policymakers.

- **Critical thinking:** Does the platform make learners explain, compare, justify or verify AI-generated answers, or does it let them accept the output as is?
- **Academic honesty:** Does the system draw a clear line between responsible AI assistance and passing AI-generated work off as one's own?
- **Teacher agency:** Can teachers override, adapt or reject AI recommendations, and are they trained to exercise that judgement?
- **Child data protection:** What student data is collected, stored and shared, and are consent and retention rules clearly defined?

- **Algorithmic transparency:** Are AI recommendations explainable to teachers, administrators and auditors?
- **Equity and meaningful access:** Are rural schools, low-income learners and teachers with weak digital skills genuinely supported?
- **Grievance and accountability:** Can students, parents and teachers challenge a wrong recommendation, a biased output or a data error?

Questions like these push DPI audit in education past technical controls and into moral, pedagogical and social ground. Skip them, and a system can pass every technical test while still being socially harmful or ethically unprepared.

## 8. Reflections for Uzbekistan

Uzbekistan is well placed to build this carefully. The digital foundations are already there: identification systems, government service portals, education management platforms and a national AI strategy. The task now is to make sure AI education tools arrive as governed systems — with ethical, pedagogical and social safeguards — rather than as efficiency upgrades.

“Pedagog yordamchi” can be one of those careful steps if three things hold. AI assists the teacher rather than replacing them. Students are taught to use AI responsibly and honestly before they are expected to use it productively. And audit and governance are built in from the start, not retrofitted after launch.

Done this way, AI in education connects technological progress with Uzbekistan’s own educational and moral values, and it is measured by human development, not just by test scores. It also opens a question I want to pursue further: how does education preserve ma’naviy-axloqiy tarbiya once AI starts to mediate the relationship between teacher, learner and knowledge?

## 9. Conclusion

DPI enables inclusive governance when it is built around trust, access and accountability. Once AI enters education, inclusion has to mean more than access to a platform. It has to include the protection of critical thinking, moral development, academic honesty, teacher agency and children’s data.

India Stack and the iCISA discussions show that architecture, safeguards and audit are what keep DPI sustainable. For AI in education, that lesson is sharper still.

The point of this article is straightforward. AI should not become the educator, nor should it quietly turn the teacher into an operator. It should remain a responsible assistant inside a morally grounded education system.

Technology supports the learning, teachers remain the human guides, and audit institutions help ensure that innovation serves citizens without eroding the values education exists to protect.

## References

Cabinet of Ministers of the Republic of Uzbekistan. (2025). *Resolution No. 425 of 10 July 2025: On measures for the implementation of priority projects in the field of artificial intelligence technologies in 2025-2026*. National Database of Legislation. https://lex.uz/en/docs/7623828

India Stack. (n.d.). *India Stack: Open APIs and digital public goods for identity, data and payments*. Retrieved June 9, 2026, from https://indiastack.org

President of the Republic of Uzbekistan. (2024). *Resolution No. PQ-358 of 14 October 2024: On approval of the Strategy for the Development of Artificial Intelligence Technologies until 2030*. National Database of Legislation. https://lex.uz/en/docs/7159258

UNESCO. (n.d.). *Readiness assessment methodology*. https://www.unesco.org/ethics-ai/en/ram

UNESCO. (2021). *Recommendation on the ethics of artificial intelligence*. United Nations Educational, Scientific and Cultural Organization. https://unesdoc.unesco.org/ark:/48223/pf0000380455

UNESCO. (2023). *Guidance for generative AI in education and research*. United Nations Educational, Scientific and Cultural Organization. https://www.unesco.org/en/articles/guidance-generative-ai-education-and-research

United Nations Development Programme [UNDP], & Office of the Secretary-General's Envoy on Technology [OSET]. (2024). *The Universal DPI Safeguards Framework: A guide to building safe and inclusive DPI for societies*. https://www.dpi-safeguards.org

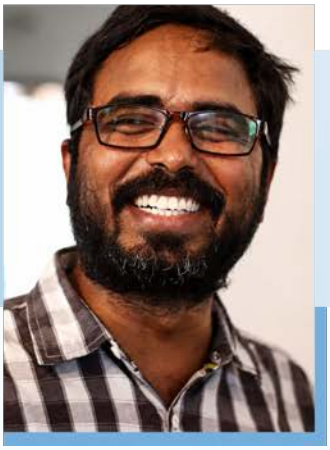


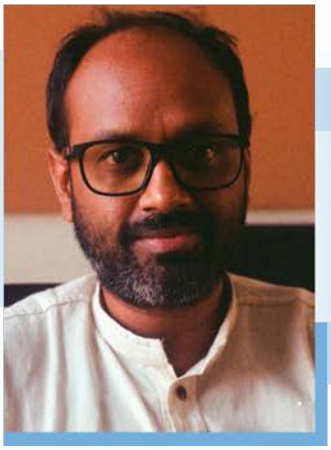
Section IV

# THE INCLUSION TEST: MAKING EXCLUSION VISIBLE AND VERIFIABLE

# Diagnosing and opening the black-box of Digital Public Infrastructure: A Process-Audit Approach to Inclusive Governance

**Chakradhar Buddha &**
**Dr. Rajendran Narayanan**
Libtech India





## Abstract

Digital Public Infrastructure (DPI) is widely promoted as an enabler of inclusive governance. Despite many positives, DPI often operates as a "black box" and results in new forms of exclusion: a benefit fails, an authentication is rejected, or a name disappears from a list, but the person cannot tell where the failure occurred, who is responsible, or how it can be corrected. This creates an audit risk: administrative success is visible on dashboards while citizen exclusion stays hidden. This article sets out a citizen-centred process-audit approach that has evolved through LibTech India's long-term work on digital welfare delivery. The approach traces a citizen's entitlement through every stage of a digital service-delivery chain and cross-checks what the system records against what the citizen actually experienced. It draws on engagement with entitlement holders, frontline workers, programme administrators and policymakers. The article presents twelve questions for auditing inclusive DPI, grouped into six dimensions and illustrated through India's digital welfare systems. Its central proposition is simple: inclusive DPI must be assessed not only from the system's point of view, but from the standpoint of the citizen.

## Keywords

Digital Public Infrastructure; Inclusive Governance; IT Audit; Process Audit; Citizen-Centric Accountability; Digital Welfare

## 1. Introduction

Digital Public Infrastructure (DPI) is increasingly shaping how public services are delivered across countries[3]. DPI refers to shared, reusable and interoperable digital systems — such as digital identity, payment platforms, databases, data-exchange layers and service-delivery portals — that can support multiple public and private services (World Bank, 2025). These are being used to deliver welfare benefits, subsidies, certificates, employment programmes and other public services. These systems promise scale, efficiency, transparency and better administrative coordination.

Notwithstanding its many positives, its proliferation needs to be balanced with a note of caution. Evidence from Andhra Pradesh's biometric payment system showed that digital reforms can reduce leakage and improve payment delivery on average (Muralidharan et al., 2016). However, there is also evidence suggesting that the Aadhaar-based payment systems have neither reduced payment delays nor reduced rejection rates (Bheemarasetti et al., 2025). Payments may be marked 'processed' but may not reach the intended bank account (Drèze, 2018), (Narayanan and Dhorajiwala, 2019). A worker may be marked absent because a mobile application meant to log workers' attendance failed (Buddha & Tamang, 2024). A worker willing to work in rural employment may not be able to, because her job card got deleted (Nair, 2023). While often dismissed as 'teething problems', in the context of rights-based welfare, digital exclusions can result in violations of rights and may also have more grievous consequences like deaths (Dutta, 2020).

In a rapidly evolving landscape of welfare delivery in India, it is therefore imperative for auditors to adapt to citizen experience and be able to track the points, reasons and scale of exclusions arising from digital mediation of welfare. For auditors, the task is to locate where the chain failed, who was affected, and whether there is a fair route for correction. A citizen-facing audit would ask whether an offline fallback exists, whether frontline workers bear device and data costs, whether failed attendance attempts are recorded, and whether workers are protected when technology fails. With these in mind, in this article, we offer a citizen-centred 'process-audit' approach that has evolved through LibTech India's work. The approach combines sustained fieldwork with large-scale data analysis. It does not propose new technologies. Rather, it offers a practical framework for examining whether DPI-enabled public services are inclusive in practice. A process audit would check whether the entitlement holder knew which bank account was linked, whether any rejection reason was communicated, and how those errors could be rectified without additional expenses.

[3] https://www.undp.org/digital/digital-public-infrastructure

For inclusive governance, the audit test is not whether the system works in ideal conditions, but whether it works for citizens facing real-world constraints such as socio-economic, geographic or digital barriers.

## 2. Why Conventional Audit Lenses Can Miss Exclusion

Any policy implementation, whether digital or paper-based, can result in inclusion errors, exclusion errors, or both. Inclusion errors take place when somebody not eligible for a scheme receives a benefit, such as a person wrongfully availing of rations under the National Food Security Act (NFSA). Exclusion errors happen when somebody eligible for a scheme does not receive its benefits, owing to administrative mistakes. Governments tend to focus on minimising inclusion errors. However, Dr B. R. Ambedkar envisioned socio-economic rights in welfare to be on par with civil and political rights. Seen from this perspective, exclusion errors are tantamount to a violation of rights and so the mode of delivery, paper-based or digital, must align to minimise exclusion errors.

Conventional audits — whether financial, compliance, performance or IT audits — examine whether funds were properly used, rules were followed, objectives were achieved and digital systems were adequately controlled.

High registrations, transactions or payments may coexist with exclusion before registration, during authentication, at payment, or during grievance redress. Digital exclusion often occurs at the last mile — in precisely the places that aggregate reports overlook. These become visible only when official records are compared with citizens' actual experience. For example, a payment dashboard may show that wages were processed. But a citizen-facing audit asks whether the worker received the money in an accessible account, knew which account was linked, understood any failure reason, and could correct the error without repeated trips or intermediaries. If an audit looks only at successful transactions, it may miss those who never completed one.

A citizen-facing auditing lens does not replace conventional audit methods but expands the evidence base. It treats failed attempts, field verification, citizen testimony, frontline worker experience and grievance journeys as important audit evidence to learn from.

## 3. Why DPI Needs a Citizen-Facing Audit Lens

The layered structure of DPI creates both opportunities and risks. If the underlying systems work well, services can be delivered at scale. But if one layer fails — through identity mismatch, biometric failure, incorrect bank linkage or poor connectivity — the citizen may be excluded even when otherwise eligible. For citizens, these layers are usually invisible. They experience the system only through its binary outcome: payment received or not received, attendance accepted or rejected, application approved or pending, name present or missing. When something fails, it is usually unclear at what layer or level it has failed. They often do not know whether the problem

lies with the local office, scheme database, identity system, bank, payment platform or service portal.

A process audit approach asks how DPI works in practice for the person who depends on it. Can they enter the system, complete the process with minimal cost, receive clear information, understand rejection reasons, correct errors, and know who is responsible when several agencies are involved?

## 4. A Process-Audit Approach

A process audit begins with the citizen's entitlement and traces the full pathway through which it is claimed, verified, delivered, denied or corrected. It treats a digital system not only as a technology platform, but as part of an administrative chain that shapes access to public services.

First, the audit starts from the right/entitlement, not the platform. The question is not simply whether the software functions, but whether the citizen can actually receive what they are entitled to — a wage, pension, ration, subsidy, certificate, licence or grievance response.

Second, understand the potential points of exclusion by mapping the service-delivery process end to end. This includes application, documentation, eligibility verification, authentication, approval, payment or delivery, communication, grievance redress and correction. The map should also identify the offices, databases, frontline workers, banks, technology vendors, service centres and any other agencies involved. This helps locate where exclusion can occur.

Third, the audit examines granular records by tracking stage-wise information: who applied, whose application was accepted or rejected, why it was rejected, whose payment was generated, whose payment failed, who raised a grievance and how they raised it, and how it was resolved if it was resolved.

Fourth, official records need to be verified against citizens' actual experiences. This is the core of the approach. Field verification can reveal missing data, such as applications or demands that were never entered into the system, and inaccurate data, such as records showing payment when the citizen did not receive or could not access the money.

Finally, the findings are consolidated to identify systemic failure points. The aim is not only to document individual grievances, but to see whether failures recur at particular stages, for particular groups, or because of particular design choices. A simple funnel — eligible, registered, approved, paid, able to access, able to resolve problems — can help show where citizens drop off.

**Figure 1:** Illustrative output from a process audit of a public housing scheme by LibTech India

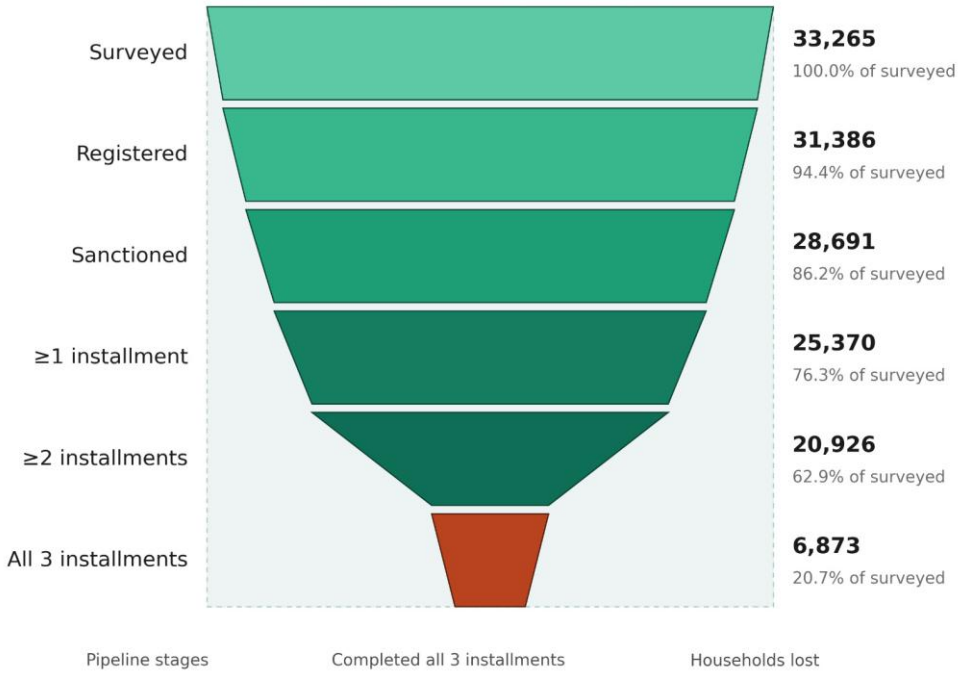



Figure 1 is drawn from a process audit of a housing welfare scheme. It traces households across successive stages of the delivery pipeline: surveyed, registered, sanctioned, and receipt of instalments. The figure shows that while most surveyed households were registered and sanctioned, only 20.7% received all three instalments. This kind of process audit helps identify where people are delayed, dropped, or excluded within a digital public infrastructure-enabled welfare system.

Such an approach triangulating system records with citizen experience helps declutter the black box of digital service delivery.

## 5. Twelve Questions for a Citizen-Facing Process Audit

The process-audit approach can be translated into twelve questions for auditing inclusive DPI. They are grouped into six dimensions and applied across the service-delivery chain.

### Legal and policy basis

- **Is the system grounded in law or stable policy?**
  Digital governance should not add conditions that weaken existing entitlements. Auditors should examine whether requirements such as authentication, digital registration or platform-based verification are in accordance with the underlying law, rules or clear policy.

### Access and cost

- **What costs does the system shift onto citizens?**
  A digital system may reduce administrative costs while increasing citizens' costs. Auditors should look for additional costs incurred by citizens in accessing rights/entitlements. Some of these costs may be implicit, such as opportunity costs. This may minimally include accounting costs for travel, mobile data, service-centre fees, extent of repeated visits, opportunity cost of losing daily wages and any additional cost for dependence on intermediaries.
- **Are assisted or offline alternatives available?**
  If the system requires documents, connectivity, smartphones, biometrics or digital literacy, there should be a viable route for those who lack them.

### Outcomes and rights

- **Does digital coverage translate into actual outcomes?**
  High registration or transaction numbers should be tested against timely payments, complete benefits and usable services. Scale should not be treated as proof of accuracy or inclusion.
- **Does the system address the real barriers citizens face?**
  A digital reform may target fraud, duplication or monitoring while citizens continue to face delays, denials, payment failures or lack of information. Auditors should compare the stated objective with citizens' actual bottlenecks.
- **Does the system help citizens claim and track entitlements?**
  Citizens should receive dated receipts, status information, reasons for rejection (if any) and timelines for action. A system that only helps administrators monitor delivery may not help citizens secure accountability.

### Exclusion and redress

- **Who is being excluded, and why?**
  Auditors should examine whether exclusion is linked to identity errors, biometric failures, data mismatches, migration, disability, remoteness, language, age, gender or lack of documents.
- **Is there a simple route back into the system?**
  The mechanisms for correction should be clear, time-bound and affordable. Exclusion becomes more serious when citizens cannot easily correct errors or re-enter the system. Protocols for correction must be well communicated to frontline officials as well.

### Data and resilience

- **Are records accurate and easy to correct?**

Wrong records can lead to loss of wages, pensions, food or subsidies. Auditors should test whether citizens can identify errors and get them corrected without unreasonable burden.

- **What happens when the system fails?**
  Auditors should outline an exhaustive typology of system failures and assess costs incurred by citizens for such failures and also examine their resolution protocols. Examples of system failures include: network failure, server downtime, biometric failure, payment rejection and breakdowns between agencies.

### Adoption and governance

- **Is adoption genuinely useful or mainly compelled?**
  High usage may reflect compulsion rather than usefulness. Auditors should ask whether citizens and frontline workers would continue using the system if meaningful alternatives existed.
- **Were affected communities and frontline workers meaningfully consulted?**
  Inclusive DPI should be shaped by those who use and implement it. Consultation during design, rollout and review can help identify exclusion risks before they become systemic.

Table 1 maps these questions to audit objectives, likely evidence sources, possible audit procedures and indicators of exclusion.

**Table 1. The twelve questions mapped to audit objectives, evidence and tests (Authors' framework)**

| Q | Audit objective | Likely evidence source | Audit test / procedure | Indicator of exclusion |
|---|---|---|---|---|
| 1 | Confirm that the entitlement rests on law or stable policy, not fragile circulars | Enabling Act and rules; circulars and notifications | Trace each digital rule to its legal source; check for conditions added by design | Entitlement weakened or conditioned by an instruction without clear legal or policy backing |
| 2 | Assess costs shifted onto citizens | Citizen interviews; fee and charge records; travel and time logs (similar to a time use survey) | Estimate cost-to-access per transaction and per citizen | Citizen spends time or money to obtain what is already due |
| 3 | Verify that an assisted or offline fallback exists | Process map; service-centre records; field observation | Attempt service completion without smartphone, connectivity or biometrics | No viable non-digital route to an essential service |

| Q | Audit objective | Likely evidence source | Audit test / procedure | Indicator of exclusion |
|---|---|---|---|---|
| 4 | Test whether coverage yields timely, complete outcomes | MIS transaction data; payment-timeline records | Funnel analysis plus timeliness measurement | High coverage with large drop-off or delay |
| 5 | Check whether the digital reform addresses the main problem citizens actually face | Grievance logs; rejection reasons; citizen accounts | Compare the stated objective against the dominant cause of failure | Reform targets fraud, duplication or monitoring while citizens continue to face denials, delays and payment failures |
| 6 | Assess whether citizens can know, claim, track and seek accountability for their entitlements | Interface review; receipts; status and notification records | Walk through the citizen-facing information flow end to end | No receipt, reason, status or timeline provided |
| 7 | Identify who is being excluded and the reasons for exclusion | Deletion and rejection records; field audits, interviews with citizens facing rejections/deletions and frontline officials | Breakdown of the failures by location, age, gender, disability, social group and reason, and verify a minimum number of cases for each reason through field visits. | Some groups/communities experience disproportionately high levels of rejection, exclusion or failure |
| 8 | Test transparency of status, reason, responsibility and deadline | Notifications; grievance portal; helpdesk records | Trace a failed case end to end to identify the reason for failure, the agency or official responsible for correction, and the deadline for resolution. Interview frontline officials on their ability/training to rectify. | Citizen cannot learn why it failed, who must fix it, or by when. |

| Q | Audit objective | Likely evidence source | Audit test / procedure | Indicator of exclusion |
|---|---|---|---|---|
| 9 | Verify data are protected and correctable | Data-correction logs; privacy and access controls | Test the ease and time taken to correct a record | Errors hard to correct; weak data protection |
| 10 | Test continuity in outages and clear cross-agency responsibility | Outage logs; service-level agreements; inter-agency arrangements | Trace a failure across agency boundaries | Citizen bounced between agencies during a failure |
| 11 | Assess whether digital adoption is genuine and equitable | Usage data disaggregated by group; citizen interviews | Analyse adoption across different social groups and ask users whether they would continue using the system if participation were optional. | Adoption only under compulsion; unequal across groups |
| 12 | Verify consultation and informed consent | Consultation records; consent and seeding records | Review participation in design and rollout, and consent obtained | Top-down imposition; no informed consent in the citizen's language |

*Source: Authors' framework, evolved from LibTech India's field-based process-audit practice.*

## 6. Methods for Public-Sector Auditors

For public-sector auditors, a process audit has implications not only for what is examined, but for how the audit is designed.

First, audit planning should begin by identifying the entitlement and the citizen groups most likely to face barriers. This helps auditors in selecting locations, transactions and user groups that can reveal the nature of systemic exclusions.

Second, audit evidence should combine administrative records with field verification. Digital records show what the system captured; citizens and frontline workers can show what the system missed, misrecorded or rejected. This is especially important where several agencies are involved. Ensure that the software interface as seen by frontline officials is captured in the auditing process and their challenges of what they can or cannot do are documented.

Third, audit teams may need to plan for methods beyond document review and system walkthroughs. Tracing a sample of failed cases end to end can provide evidence that dashboards alone cannot show. Such evidence can also inform the design of national household surveys, which rarely ask whether an entitlement was claimed but never received.

Fourth, audit reporting should make the accountability chain visible. Where exclusion occurs, the report should identify the stage of failure, the affected groups, the agency responsible for correction, and the changes needed to prevent recurrence.

Finally, the audit report should provide detailed methodologies used by governments in arriving at savings due to digital innovation. This would help in better planning and allocation of resources for welfare.

In this sense, a citizen-facing process audit helps public-sector auditors move from asking whether a digital system functions to whether it enables access, correction and accountability in practice.

## 7. Conclusion

DPI can strengthen inclusive governance, but inclusion is not automatic. A system may be efficient and exclusionary at the same time: generating dashboards without accountability, transactions without access, and automation without explanation. The black-box problem is therefore central to auditing DPI. Effective accountability rests on citizens' ability to know why they were excluded, where the failure occurred, who is responsible, or how it can be corrected.

This article has proposed a citizen-centred process-audit approach for diagnosing and opening the DPI black-box. It begins with the entitlement, maps the service-delivery chain, examines granular records, verifies them with citizens, and identifies systemic failure points. The twelve questions help auditors ask whether DPI-enabled services are accessible, affordable, outcome-oriented, explainable, correctable, resilient and accountable.

The central test is simple: does the system work for the citizen most likely to be excluded? If an audit cannot answer that question, the black box remains closed.

## References


1. Bheemarasetti, S., De, A., Narayanan, R., Saboo, P., & Tamang, L. (2025). MGNREGA as a technological laboratory: Analysing wage payment delays as a result of two digital interventions. *The Indian Journal of Labour Economics, 68*(2), 681–706. https://doi.org/10.1007/s41027-024-00539-9
2. Buddha, C., & Tamang, L. (2024). MGNREGA's attendance app: A tool for transparency or exclusion? *Economic & Political Weekly, 59*(48). https://www.epw.in/journal/2024/48/commentary/mgnregas-attendance-app.html
3. Drèze, J. (2018, August 3). Done by Aadhaar. *The Telegraph.* https://www.telegraphindia.com/opinion/done-by-aadhaar/cid/1467855
4. Dutta, S. (2020). *Starvation deaths and denial of welfare entitlements: Insights from Jharkhand* [Working paper]. SSRN. https://doi.org/10.2139/ssrn.3870242

5. Muralidharan, K., Niehaus, P., & Sukhtankar, S. (2016). Building state capacity: Evidence from biometric smartcards in India. *American Economic Review, 106*(10), 2895–2929.
6. Nair, S. (2023, June 25). Job card–Aadhaar mismatch: A missing letter means no work for MGNREGS workers in Odisha. *The Hindu.* https://www.thehindu.com/news/national/job-card-aadhaar-mismatch-a-missing-letter-means-no-work-for-mgnregs-workers-in-odisha/article67005710.ece
7. Narayanan, R., & Dhorajiwala, S. (2019). The namesake: Human costs of digital identities. *Economic & Political Weekly Engage, 54*(49). https://www.epw.in/engage/article/namesake-human-costs-digital-identities
8. World Bank. (2025). *Digital public infrastructure and development: A World Bank Group approach.* World Bank. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099031025172027713

# Inclusion by Verification: Why Digital Public Infrastructure's Promise of Inclusive Governance Depends on a Dedicated Data-Reliability Audit Approach

**Jishnu J Raju**
O/o the Comptroller & Auditor General of India



## Keywords

Digital Public Infrastructure, inclusive governance, data reliability, government audit, Aadhaar, exclusion error, audit-by-design

## 1. Introduction

Digital Public Infrastructure has moved, in the space of a few years, from a description of India's own technology stack to a term of art in global development policy. The United Nations Development Programme describes DPI as a set of foundational digital systems — digital identity, payments, and data exchange — that forms the backbone of modern societies, enabling secure and seamless interactions between people, businesses, and governments, and making everyday life "more connected and inclusive" (UNDP, Digital public infrastructure). The World Bank frames DPI in almost identical terms: shared, interoperable platforms, akin to physical highways or bridges, that reduce duplication and allow both public and private actors to scale services — with the explicit warning that, absence of such infrastructure, "digitalization risks reproducing existing inequalities in access to services, jobs, and economic opportunities" (World Bank, Digital Public Infrastructure and Services). Under India's 2023 G20 Presidency, this vision was formalised for the first time in a common intergovernmental description, with the G20 New Delhi Leaders' Declaration describing DPI as a set of shared digital systems, secure and interoperable, built on open standards, that deliver equitable access to public and private services at societal scale (G20 New Delhi Leaders' Declaration 2023). The UN Secretary-General has since named DPI one of twelve high-impact initiatives selected to accelerate the Sustainable Development Goals (UNDP, G20 Digital Ministers Recognize Digital Public Infrastructure), and the 50-in-5 campaign — a joint effort of UNDP, the Gates Foundation, UNICEF, and partner governments — has set out to help fifty countries design, launch, and scale at least one DPI component "in a safe, inclusive, and interoperable manner" by 2028 (50-in-5, Implementing digital public infrastructure, safely and inclusively).

The theme uniting this literature is inclusion. DPI is advocated for not merely as a more efficient way to run existing government systems, but as a mechanism capable of reaching citizens whom paper-based, fragmented, or discretionary systems have historically excluded: the rural resident without a bank branch nearby, the informal worker without a stable address, the elderly pensioner without documentary proof of identity. Brazil's CadÚnico unified registry of low-income families, cited by UNDP as a flagship example of inclusive DPI, is explicitly designed around this logic — using a shared digital identity layer to bring previously undocumented households into the reach of social protection (UNDP, UN Digital event mobilizes global leadership). The claim, in short, is that DPI is an enabler of inclusive governance: it expands who the state can see, serve, and be accountable to.

This article does not dispute that claim. It argues instead that the claim is conditional in a way the DPI literature has so far under-examined. A digital identity or payment system enables inclusion only if it correctly recognises the people it is meant to include, and correctly denies itself to anyone who is not entitled to its benefit. Whether it does so is, at bottom, an empirical question about the reliability of the data the system produces and consumes — and empirical questions of this kind are precisely what the audit function exists to answer independently, rather than take on the system owner's own assurance. Where a DPI system's data cannot be independently verified, “inclusive governance” and its opposite are, from the outside, indistinguishable: the system may be quietly including everyone it should, or quietly excluding a meaningful share of the very citizens it was built to reach, and neither citizens, legislatures, nor development partners funding the 50-in-5 campaign would necessarily be able to tell the difference. Independent, evidence-based audit — specifically, audit of the reliability of DPI data — is therefore not an afterthought to DPI's inclusion agenda. It is one of the load-bearing conditions on which that agenda depends.

This article's central claim is that the audit methodology developed for the government information systems that inclusive-DPI advocates are used to examining does not transfer cleanly to DPI itself. DPI is not simply a larger database; it is a system of systems — a federated, API-mediated, population-scale architecture in which no single actor, including the audited entity, necessarily holds a complete, authoritative account of how a given data point came to be what it is. Auditing such a system with tools built for a single application running on a single server risks two failure modes, each with direct consequences for the inclusion agenda: either the audit concludes, correctly but unhelpfully, that DPI data are of “undetermined reliability” because access and documentation cannot be assembled within the audit's usual scope and timeline — leaving the inclusion claim unverified either way; or the audit applies conventional sampling and tracing techniques that were never designed to catch the class of error — systemic exclusion arising from biometric mismatch, for instance — that matters most to the citizens DPI is meant to reach. Either way, the audit function falls short of what “inclusive governance” requires it to establish.

The remainder of the article proceeds as follows. Section 2 sets out, in more detail, why the global DPI-for-inclusion literature treats data reliability as an audit precondition for its own claims, even where it does not use that language. Section 3 develops five specific points of mismatch between conventional data reliability assessment and DPI. Section 4 examines what the CAG's own 2021 performance audit of the Unique Identification Authority of India (UIDAI) already reveals about these mismatches in practice, and what they mean for inclusion outcomes specifically. Section 5 proposes elements of a dedicated DPI audit approach. Section 6 considers what this means for the reliability determination itself. Section 7 concludes by returning to the inclusive-governance framing directly.

## 2. Inclusion as an Empirical Claim, Not a Design Feature

It is worth being precise about what "inclusive" means in the DPI literature, because the term is doing real analytical work, not just rhetorical work. The World Bank Group's 2025 DPI framework paper lists inclusion, alongside interoperability, security, and governance for public benefit, as one of the core design principles a system must embed to qualify as DPI at all (World Bank Group, Digital Public Infrastructure and Development). The G20 Digital Economy Working Group's own principles for DPI, adopted in 2023, likewise name inclusivity as a first-order design requirement, alongside interoperability, security and privacy, and governance for public benefit, trust, and transparency (World Bank Group, Digital Public Infrastructure and Development, citing G20 DEWG 2023). The 50-in-5 campaign goes further, arguing that DPI built without safeguards for safety and inclusion risks higher retrofitting costs later, and that "safety and inclusion are the foundation for DPI uptake and innovation" (50-in-5, Putting safeguards into action) — a claim echoed in the UN's own Universal DPI Safeguards Initiative, launched by the Secretary-General's Envoy on Technology alongside UNDP specifically to address the risk that DPI, unsafeguarded, could reproduce or deepen exclusion rather than remedy it (UNDP, UN Digital event mobilizes global leadership).

What is notable across this literature is that inclusion is treated, consistently, as a design intention — something DPI should embed, is meant to embed, is built to embed — rather than as a claim that has itself been independently verified against outcomes for the specific citizens a given system was meant to reach. This is not a criticism of the literature's sincerity; it reflects the fact that verifying an inclusion claim empirically is a different kind of exercise from stating it as a design principle, and requires a different institutional actor — one independent of the system's designers, funders, and operators — to carry it out. That actor, in most jurisdictions, is the Supreme Audit Institution.

This is where data reliability assessment and inclusive governance meet directly. A claim that a digital identity system "enables access to services and exercise of rights" (the World Bank's ID4D mission statement, quoted in World Bank Group, Digital Public Infrastructure and Development) is, formally, an empirical claim about a population: that the system correctly recognises the

people entitled to those rights, at an acceptable rate of error, across the specific groups the system was intended to reach. An audit party assessing the reliability of that system's authentication data is, in substance, testing this inclusion claim directly — not as a side effect of a routine compliance exercise, but as the central empirical question the inclusion literature itself raises and does not, on its own, answer. Sections 3 through 6 of this article are therefore not a detour from the theme of DPI as an enabler of inclusive governance; they are an argument that data reliability audit is the mechanism by which that theme's central claim can be tested, rather than merely asserted.

## 3. The Structural Mismatch: Why Conventional Data-Reliability Audit Falls Short for DPI

Four features of DPI's architecture matter for audit purposes, and each one breaks an assumption implicit in conventional data reliability guidance of the kind long used by Supreme Audit Institutions, including the U.S. Government Accountability Office's own Assessing Data Reliability guide (GAO 2019).

DPI is federated by design. No single application “owns” an identity-linked welfare transaction end to end. A single disbursal under a direct benefit transfer scheme typically passes through a scheme database, a beneficiary-management system, a public financial management platform, a payment bridge or instant-payment rail, the recipient's bank, and a national payment-switching infrastructure — with the identity layer invoked at one or more points for authentication. Conventional data reliability assessment assumes an identifiable “data owner” who can be interviewed and whose system can be tested. DPI routinely presents an audit party with five or six such owners for a single transaction, each holding a partial and differently structured record of the same underlying event.

DPI is explicitly built to operate at population scale. The G20's own definition frames DPI's promise in exactly these terms: a set of shared digital systems, secure and interoperable and built on open technologies, meant to deliver equitable access to public and/or private services at a societal scale (G20 New Delhi Leaders' Declaration 2023). A government information system examined under conventional audit methodology might hold a few million records; DPI systems process hundreds of millions of transactions a month. At that scale, an error rate that would be immaterial in a conventional dataset — a fraction of one percent — translates into an inclusion or exclusion outcome for a very large number of citizens, a magnitude problem the existing materiality and risk framework was not built to calibrate against.

DPI relies on algorithmic and biometric matching as a core function, not an incidental feature. Deduplication, liveness detection, and fingerprint or iris matching are the mechanisms by which the system decides whether a transaction is valid at all. This introduces a class of error — probabilistic mismatch rather than binary presence or absence of a value — that sits awkwardly

within the “missing data / duplicate records / out-of-range values” vocabulary of conventional data testing, yet is precisely the error type most likely to produce the exclusion outcomes the inclusive-DPI literature is trying to guard against.

DPI's governance model deliberately brings private and quasi-private intermediaries inside the data supply chain. Authenticating agencies, requesting entities, banks, and payment aggregators are, by design, part of how DPI data comes into being, yet most sit outside the direct audit jurisdiction that applies to a government department. A regulator that cannot compel and verify assurance over the private intermediaries inside its own DPI ecosystem leaves an SAI examining the same terrain facing the identical jurisdictional gap, compounded.

## 3.1 Population scale turns small error rates into large absolute exclusion harms

A useful illustration comes from the debate over biometric authentication in a large public distribution system. Independent field studies have found an average state-wide authentication failure rate of around 2.5 percent in one Indian state, rising above 5 percent in some districts, with roughly 92 percent of those failures attributable to biometric mismatch rather than missing enrolment data (Chhatre, ISB study on Andhra Pradesh PDS). More recent reporting has put the national monthly failure rate at a broadly similar order of magnitude: roughly 312 million biometric authentications are attempted monthly against welfare, banking, and public services, of which around 20.3 million fail, a rate that has stayed largely unchanged for a decade (Policy Circle 2026). A national-scale randomised evaluation in the Indian state of Jharkhand documented measurable rates of exclusion attributable specifically to the introduction of biometric authentication — roughly 1 percent in a public works employment guarantee scheme, 0.5 percent in pensions, and 1.5 percent in the public distribution system — each smaller than exclusion from pre-existing administrative error, but still affecting a substantial absolute number of the very citizens the underlying schemes exist to include (NCAER 2022). In a conventional government dataset of a few thousand records, error rates in this range would likely fall within an “acceptable” band under existing reliability guidance. Applied to a system processing hundreds of millions of monthly transactions, the same percentage becomes an exclusion finding in its own right — arguably more consequential to the inclusive-governance claim than anything else the audit could report.

## 3.2 Algorithmic matching as a distinct error class

This pattern is serious enough that it was raised across party lines when Parliament's Public Accounts Committee examined the CAG's 2021 UIDAI report, with committee members noting that many labourers' worn fingerprints and elderly citizens' changed iris patterns no longer matched enrolment records, resulting in wrongful exclusions (Biometric Update 2025). A

duplicate-record check or a range check will not reveal this kind of failure; assessing the reliability of an algorithmic matching function requires testing the matching engine itself against known inputs and examining false-rejection design and fallback procedures — a toolkit closer to model or system assurance than to "trace a sample of records to source vouchers."

### 3.3 Private intermediaries inside the data supply chain, outside audit jurisdiction

The CAG's 2021 performance audit of UIDAI documented this gap directly: UIDAI, as regulator, had not established a defined encryption standard for the data vaults that authenticating entities were required to maintain, leaving compliance to the entities' own self-certification, and had not itself verified that certification — the audit found that no authentication service agencies had their own operations independently audited annually as required (CAG Report No. 24 of 2021, via MediaNama 2022).

### 3.4 Continuous, real-time flows that outrun periodic audit cycles

DPI is designed to operate continuously, across a live population whose underlying facts are themselves constantly changing. UIDAI's own exercise to deactivate the identity numbers of deceased persons illustrates the scale of this churn: as of mid-2025 the authority had received on the order of 15.5 million death records from the civil registration system across 24 states and union territories and had deactivated roughly 11.7 million corresponding numbers on that basis, with a further roughly 670,000 records from non-integrated states under verification (Biometric Update 2025). A dataset that changes materially every day cannot be fully captured by the single point-in-time extract conventional guidance implicitly assumes.

## 4. What the CAG's Own Audit of UIDAI Already Shows About Inclusion

The CAG's 2021 performance audit of UIDAI, covering 2014-15 to 2018-19, is an early and instructive attempt to grapple with exactly this terrain — and its findings illustrate the structural mismatch from the inside, with a direct bearing on the inclusion question. The audit reported that UIDAI had to cancel more than 475,000 identity numbers, as of November 2019, for being duplicates — indicating that, on average, no fewer than 145 duplicate numbers were generated per day over the system's first nine years (CAG Report No. 24 of 2021, via Drishti IAS) — a finding that speaks directly to how difficult it is, even for the system's own regulator, to maintain a single authoritative identity record at population scale, which is itself the precondition for the "one person, one entitlement" logic on which inclusive service delivery depends. The audit's findings on undefined vault-encryption standards and near-absence independent audits of authentication agencies show the private-intermediary gap described in Section 3.3. And the audit team's own account of conducting the review records that requisitioned records were generally furnished, but that the audit "witnessed several instances of inordinate delay or non-

supply," including files relating to the authentication ecosystem and the accounting of authentications themselves (CAG Report No. 24 of 2021) — a direct, first-hand illustration of the access friction described in Section 3.

That these issues surfaced years before the Public Accounts Committee's 2025 follow-up, and that the committee found broadly similar authentication-failure concerns still live at that later date (Biometric Update 2025), suggests two things relevant to the inclusive-governance theme specifically. First, a one-off performance audit, however well executed, is not by itself a sufficient response to a problem that is structurally continuous, for the reasons given in Section 3.4. Second, and more fundamentally: the specific gaps this audit found — an imperfect single system of record, unverified private-intermediary assurance, and access friction — are not incidental implementation bugs to be fixed in the next system upgrade. They are the direct mechanism by which a DPI system's stated design intention of inclusion can silently fail to translate into inclusion outcomes for specific citizens, exactly as Section 2 anticipates.

## 5. Toward a Dedicated DPI Audit Approach

If the mismatches above are taken seriously, a dedicated DPI audit approach needs to depart from conventional data reliability methodology in six specific respects.

First, system-of-systems mapping should precede technique selection. Before choosing among interviews, documentation review, testing, or tracing, the audit party needs to map the full chain of systems and institutions through which a given class of DPI data passes, identifying which entity holds which partial record and where reconciliation between them does, or does not, occur.

Second, audit access needs to be built into DPI governance instruments themselves. The CAG's own experience of delayed and partial access to UIDAI records suggests that access to a federated, partly privatised ecosystem cannot reliably be secured through case-by-case documentation requests. Regulatory instruments governing DPI intermediaries should build in a standing audit-access right for the SAI, comparable to the access rights that already attach to bodies substantially financed by government.

Third, DPI audit needs continuous or near-continuous assurance techniques, not only periodic ex-post sampling. Given the churn documented in Section 3.4, a periodic point-in-time reliability determination has a naturally short shelf life. Embedded, API-based test harnesses — automated queries run at defined intervals against production or near-production data — would allow an SAI to monitor indicators such as authentication failure rates on an ongoing basis rather than discovering drift only at the next full audit cycle.

Fourth, DPI audits crossing jurisdictional and public-private boundaries call for coordinated, joint audit arrangements as the default. SAIs already have traditions of coordinated audits across subnational offices for schemes with a national footprint; DPI's federated architecture, spanning national nodal agencies, subnational departments, and private intermediaries simultaneously, is close to a paradigm case for extending that tradition.

Fifth, “transaction accuracy” and “outcome reliability” need to be treated as analytically distinct audit questions. A payment can be entirely accurate as a transaction — the right amount moved to the right account, correctly logged — while the underlying eligibility determination that triggered it was wrong, or while an eligible citizen was excluded because an upstream authentication step failed. Conventional data testing is well suited to the first question and poorly suited to the second, yet the second is the one on which the inclusive-governance claim actually rests.

Sixth, exclusion error should be treated as a first-class risk category in its own right. Failures disproportionately affect the same vulnerable groups the underlying schemes exist to serve, and are structurally likely to be under-reported precisely because they manifest as an absence — a person who never appears in the data at all — rather than as a visible error in an existing record. When exclusion occurs, no single agency owns the outcome, and there is typically no systematic tracking of exception use, success rates, or outcomes, since a failure simply disappears from the system once it moves outside the biometric logs that would otherwise register it (Policy Circle 2026). Existing guidance's completeness criterion does not, on its own, direct an audit party to actively search for people who should be present in a beneficiary dataset but are not; a dedicated DPI approach should require exactly this kind of active, outcome-oriented search, comparing system data against an independent population benchmark, as a standard step rather than an optional enhancement.

## 6. Implications for the Reliability Determination Itself

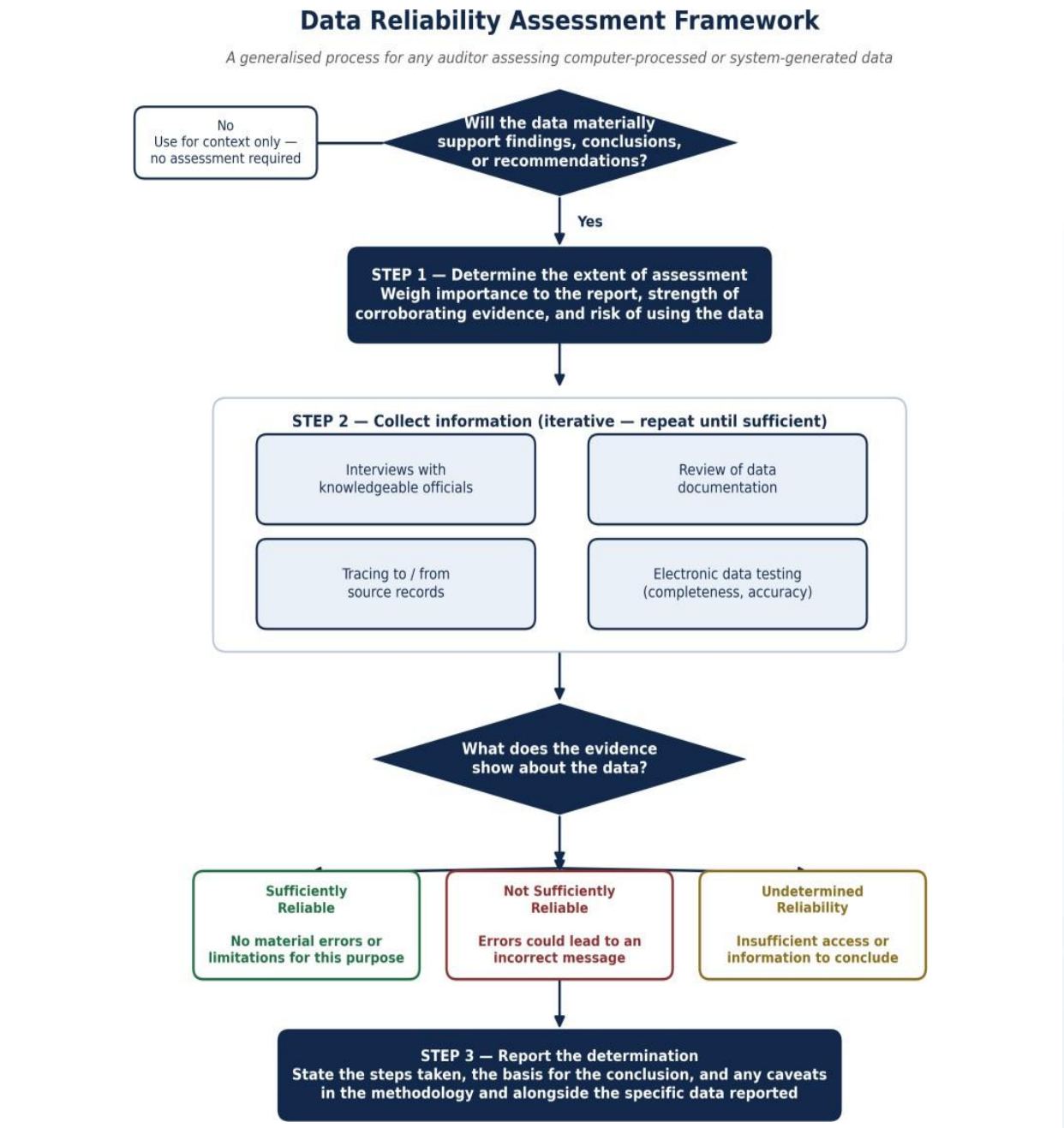



*Figure 1. The conventional data reliability assessment framework: a trigger question, a risk-sized scope, an iterative evidence cycle across four techniques, and a three-way determination. Adapted from GAO (2019) and comparable Supreme Audit Institution guidance. As Sections 3–6 argue, each stage of this sequence — access for the evidence cycle, and the meaning of "undetermined" in the final determination — needs to be re-examined for Digital Public Infrastructure specifically.*

These six elements bear directly on how the conventional sufficiently-reliable / not-sufficiently-reliable / undetermined-reliability trichotomy should be applied to DPI. Under a conventional reading, an audit party facing a federated system with partial access, a poorly defined system of record, and reconciliation gaps between institutions would very often be pushed, entirely

reasonably, toward a determination of undetermined reliability. Applied consistently to DPI, this would mean that a large and growing share of the data now underpinning welfare delivery and financial inclusion worldwide would formally sit in the "undetermined" category for audit purposes — not because the data are demonstrably unreliable, but because the audit apparatus available to test them was not built for a system of this shape.

For a body of infrastructure whose entire policy justification is inclusive governance, this is not a satisfactory resting point. "Undetermined reliability" reads, in a report, as a hedge — a statement that the audit party could not reach a conclusion — when the more accurate and more consequential statement, in many DPI cases, is that the system as currently governed does not yet support the kind of independent verification that an "inclusive" and "trusted" infrastructure claim requires. The constructive response is to treat the conditions that produce an undetermined determination — absent audit-access guarantees, absent standing continuous-assurance mechanisms, absent a clearly designated system of record — as themselves a distinct class of finding, with the recommendation attached to the DPI governance framework rather than to the specific dataset examined in a single engagement. Where a data reliability assessment of a DPI component would otherwise land on "undetermined," the audit party has a strong case for reporting that outcome as a governance finding in its own right: that the system has not been designed to be independently auditable, and that this is itself a barrier to verifying the inclusion claim made on the system's behalf.

## 7. Conclusion: Returning to Inclusive Governance

DPI's central promise, repeated across the UNDP, World Bank, G20, and 50-in-5 literature surveyed in Section 2, is that shared digital infrastructure can reach citizens whom earlier, fragmented systems left out — that it can be, in the terms the theme of this issue sets out, an enabler of inclusive governance. This article has not challenged that promise. It has argued that the promise is an empirical claim, not a design feature, and that empirical claims of this kind require independent verification to be more than an assertion. Conventional data reliability assessment, developed for discrete government information systems with an identifiable owner, a bounded population of records, and a periodic extract as the natural unit of analysis, does not transfer cleanly to DPI's federated, population-scale, algorithmically mediated, continuously operating architecture — and the gap matters most exactly where the inclusion claim matters most: at the point where a citizen's biometric, identity, or eligibility record is matched, or fails to match, against a system of record no single institution fully owns.

The CAG's own 2021 performance audit of UIDAI illustrates both the value and the limits of applying existing methodology to this terrain: it surfaced genuinely important findings — on duplicate identities, on undefined encryption standards for private intermediaries, on poor compliance with the regulator's own audit requirements — while also encountering, directly, the access and system-of-record problems this article identifies as structural rather than incidental. A dedicated DPI audit approach, built around system-of-systems mapping, statutory audit-access

guarantees, continuous assurance techniques, coordinated cross-jurisdiction audit arrangements, an explicit separation of transaction accuracy from outcome reliability, and first-class treatment of exclusion error, would allow Supreme Audit Institutions to move DPI data reliability determinations out of the residual "undetermined" category and toward genuine, verifiable assurance — or, where that assurance cannot yet be given, toward a clear and actionable finding that says so.

As the 50-in-5 campaign and comparable initiatives work to help fifty countries build DPI "safely and inclusively" by 2028, the audit question this article has raised travels with that ambition. Digital public infrastructure built without corresponding attention to how its data can be independently verified is, whatever else it achieves, not yet the fully inclusive infrastructure its own advocates claim it to be. Building that verifiability in from the start — audit-by-design, alongside privacy-by-design, interoperability-by-design, and the safeguards-by-design principles the DPI Safeguards Initiative already champions — is not a constraint on DPI's inclusion agenda. It is what would allow that agenda to be trusted, and to be true.

## References


Biometric Update. (2025). High rates of Aadhaar biometric verification failure leads to UIDAI scrutiny.

Comptroller and Auditor General of India (CAG). (2021). Performance Audit on the Functioning of the Unique Identification Authority of India, Report No. 24 of 2021.

Drishti IAS. (2022). CAG report on UIDAI functioning [summary of Report No. 24 of 2021].

G20 New Delhi Leaders' Declaration. (2023). New Delhi: Government of India, G20 Presidency.

MediaNama. (2022). Is Aadhaar data being sufficiently protected by UIDAI? Here's what CAG report says.

National Council of Applied Economic Research (NCAER). (2022). Integrating Biometric Authentication in India's Welfare Programs.

Policy Circle. (2026). Aadhaar authentication failures trigger an invisible exclusion crisis.

50-in-5. (n.d.). Implementing digital public infrastructure, safely and inclusively. https://50in5.net/

50-in-5. (2025). Putting safeguards into action: 50-in-5 and DPI Safeguards Initiative launch accelerator for countries. https://50in5.net/putting-safeguards-into-action-50-in-5-and-dpi-safeguards-initiative-launch-accelerator-for-countries/

United Nations Development Programme (UNDP). (n.d.). Digital public infrastructure. https://www.undp.org/digital/digital-public-infrastructure

United Nations Development Programme (UNDP). (2023). G20 Digital Ministers Recognize Digital Public Infrastructure as an Accelerator of the Global Goals. https://www.undp.org/press-releases/g20-digital-ministers-recognize-digital-public-infrastructure-accelerator-global-goals

United Nations Development Programme (UNDP). (2023). UN Digital event mobilizes global leadership and US$400 million to support digital public infrastructure. https://www.undp.org/press-releases/un-digital-event-mobilizes-global-leadership-and-us400-million-support-digital-public-infrastructure

U.S. Government Accountability Office (GAO). (2019). Assessing Data Reliability (GAO-20-283G). Washington, DC: GAO, Applied Research and Methods.

World Bank Group. (2025). Digital Public Infrastructure and Development: A World Bank Group Approach.

Digital Transformation White Paper, Volume 1. Washington, DC: World Bank.

World Bank Group. (n.d.). Digital Public Infrastructure and Services. https://www.worldbank.org/ext/en/topic/digital-and-ai/digital-public-infrastructure-and-services

Chhatre, A. et al. Indian School of Business (ISB). Biometric authentication failure study, Andhra Pradesh Public Distribution System [field study cited in secondary reporting].

# Extending the Use of Audit Data Can Help Strengthen Inclusivity

**Sandeep Radhakrishnan**
Senior Associate, Artha Global, India



## Abstract

Digital Public Infrastructure (DPI) is increasingly promoted as a means of delivering more inclusive, safe, and efficient public services. However, existing audit approaches primarily assess financial regularity, regulatory compliance, technical integrity, and value for money, without systematically examining whether DPI-enabled services are reaching the populations they are intended to serve. This article argues that inclusion should be treated as a core audit objective and that Supreme Audit Institutions (SAIs) are well placed to address it through performance auditing. It contends that achieving this requires expanding current audit practices by systematically cross-referencing audit outputs and underlying DPI operational data with sectoral administrative datasets, including demographic, welfare, health, and connectivity records. Drawing on the INTOSAI audit framework, the Public Expenditure and Financial Accountability (PEFA) framework, the UNDP–ODET Universal DPI Safeguards Framework, OECD evidence on government interoperability, and empirical studies of India's Aadhaar-enabled Public Distribution System, the article demonstrates that institutional fragmentation in data governance remains a significant barrier to verifying inclusion outcomes. While DPI is designed to overcome silos in service delivery, oversight and audit architectures remain similarly fragmented, limiting the ability of auditors to identify who is excluded and why. The article concludes by proposing a governance framework for responsible cross-referencing based on institutional coordination, purpose limitation, privacy-preserving analytics, independent oversight, and transparency. It argues that strengthening audit in this way represents a natural evolution of the SAI mandate and would enable governments to assess not only whether DPI systems function effectively, but whether they fulfil their central public purpose of inclusive service delivery.

## Introduction

Digital Public Infrastructure (DPI) is often described, and increasingly funded, as a new generation of public service delivery technology designed to maximise inclusion, with safety and security built into its design. These societal goals are among the primary reasons for public investment in digital identity, payments, and data exchange layers. Such systems are expected to reach people that older paper-based or fragmented systems could not, while doing so safely and securely.

Auditing these goals requires more than checking that a DPI system functions as specified or that public funds were spent according to the rules. It requires answering a broader question about inclusion: whether a welfare programme using these DPI systems is serving its intended population and whether any groups face disproportionate risks of exclusion.

Performance audits already provide a flexible framework for examining such questions. Under the INTOSAI Performance Audit Principles (ISSAI 300) and Performance Audit Standard (ISSAI 3000), audit objectives, criteria, evidence and materiality are determined by the specific audit questions rather than by a fixed methodology. Performance audits may adopt a system, result, or problem-oriented approach depending on the audit questions, while audit criteria may be drawn from diverse qualitative and quantitative sources. Evidence may be obtained using a range of methods, and the process can extend beyond financial accounting to include issues of social importance. SAIs across the INTOSAI community have already begun applying this flexibility to SDG-linked audits internationally — the INTOSAI Development Initiative's SDGs Audit Model (ISAM) has supported cooperative performance audits involving 49 SAIs across five INTOSAI regions, covering themes such as "Strong and Resilient Health Systems" (SDG 3.d), "Sustainable Public Procurement Using Data Analytics" (SDG 12.7), and "Elimination of Intimate Partner Violence Against Women" (SDG 5.2). Kenya, for instance, developed an SDG Recovery and Acceleration Strategy through a multi stakeholder process to overcome implementation bottlenecks, illustrating how national audit and accountability efforts have been embedded directly into whole-of-government SDG delivery. These precedents show that whole-of-government, cross-institutional performance audits geared toward inclusion outcomes are not a hypothetical extension of SAI practice but an established and growing body of international audit work.

The Universal DPI Safeguards Framework can complement this audit practice by articulating practical indicators for assessing whether DPI systems can deliver inclusion, safety and security in practice. Additionally, can the DPI performance audits that Supreme Audit Institutions (SAIs) already conduct be extended to answer questions about inclusion? Doing so would be a natural fit with the SAI mandate rather than an extension beyond it, given SAIs' own stated commitment to the "leave no one behind" principle.

Operationalising this approach requires combining different forms of data and evidence. Performance audits generate data on transaction failures, regulatory compliance, security incidents, and service quality, which can be cross-referenced with data held by other ministries and agencies on the populations these systems are intended to serve. Such data may include demographic records, welfare beneficiary rolls, health and disability records, and connectivity maps, enabling auditors to assess whether exclusion is concentrated among particular population groups and to identify the factors contributing to those outcomes.

## Audit Data in the Context of DPI

Audit data is not the operational data generated by a DPI system itself, but the evidence and findings produced through the audit process. The continuously generated "digital exhaust" from DPI systems - authentication logs, transaction records, exception reports, system alerts, and related operational data - provides a new and potentially rich source of audit evidence, particularly for performance audits. On its own, however, this data reveals how a system functions rather than whom it serves.

For performance audits examining whether public programmes are achieving their intended outcomes, the value of DPI-generated operational data lies in its ability to be linked with the sectoral administrative data held by implementing ministries. Cross-referencing authentication records with beneficiary databases, demographic information, or service delivery records can help auditors identify patterns of exclusion, understand who is being left behind, and distinguish between technical failures, administrative bottlenecks, and policy design issues. Yet these data remain institutionally fragmented, with DPI operators and sector ministries typically maintaining separate, non-interoperable systems.

This distinction is important. The digital exhaust produced by DPI systems is not itself audit output; rather, it is an emerging source of evidence that, when combined with sectoral data, can strengthen performance audits by enabling more robust assessments of whether digitally enabled public programmes are achieving their intended inclusion objectives.

## Why DPI Requires a Different Approach to Audit

This limitation matters more for DPI than for most other technology systems because of what DPI is specifically designed to do. The Universal DPI Safeguards Framework, developed by the United Nations Development Programme (UNDP) and the UN Office for Digital and Emerging Technologies (ODET), identifies three broad categories of risk: safety, inclusion, and structural vulnerabilities. It treats both safety and inclusion as core design objectives of DPI (UNDP & ODET, 2024).

The OECD's *Digital Government Outlook 2026* makes a closely related point about why DPI exists as a concept. Historically, government institutions have developed and maintained their own

digital systems in isolation, with limited incentives to integrate. DPI represents a deliberate shift towards shared, cross-ministry digital components that enable information to flow across institutional boundaries (OECD, 2026).

This is what makes the audit data problem distinctly a DPI problem rather than simply a question of audit scope. If the core justification for DPI is that it breaks down institutional silos in service delivery, then verifying whether it is achieving that objective is itself a cross-institutional exercise. It requires data generated through audits of DPI systems to be read alongside data held by the ministries whose services those systems are intended to connect. Yet the same institutional fragmentation that DPI seeks to overcome in service delivery remains largely intact in the oversight and audit architecture.

This is precisely the pattern the UN DESA's World Public Sector Report 2025 documents when examining how SAIs actually try to evaluate cross-cutting government objectives like the SDGs. In public debt audits, the report identifies "poor interoperability and integration of records and data systems used by different entities responsible for debt recording" as a recurring finding across 58 findings in 32 audit reports from 16 countries, with debt information systems often "operating in isolation from broader public administration systems" — illustrated by Indonesia's use of three separate, uncoordinated monitoring systems for budget execution and planning, which produced inconsistencies between budget ceilings and actual expenditures. The same problem recurs in climate audits, where "climate-related data is often incomplete, unreliable or scattered across multiple institutions" due to "limited information exchange and coordination tools and systems" between government bodies, and in equity audits, where SAIs have had to recommend building the very integration mechanisms DPI is meant to provide — SAI Latvia calling for a "single implementation mechanism" for poverty reduction, and SAI Lithuania for "an integrated system for assessing individual needs" for persons with disabilities, precisely because no cross-institutional data view existed (United Nations Department of Economic and Social Affairs [UN DESA], 2025).

## The Coordination Gap

The same report finds that while SAIs worldwide are increasingly incorporating the "leave no one behind" principle into their work, there exist common obstacles to auditing this principle, including the absence of systematic monitoring, poor data availability and management, and inadequate use of information in planning. The report attributes these challenges, in part, to weak institutional coordination between audit bodies and the public entities that hold the relevant data (United Nations Department of Economic and Social Affairs [UN DESA], 2025).

The OECD's Digital Government Outlook 2026 provides a more direct, quantitative picture of the underlying technical gap. Interoperability systems, the shared technical platforms that enable data exchange across government institutions, are in place in 30 of the 36 OECD member countries. However, only 23 of those 30 countries report widespread use of these systems,

defined as adoption across more than half of central government institutions. This suggests that, even where the technical infrastructure exists, broad institutional adoption remains incomplete. Adoption at the subnational level of government is lower still (OECD, 2026). If cross-government data interoperability remains incomplete in the world's most digitally advanced governments, the specific, purpose-built linkage needed to cross-reference DPI audit data with sectoral ministry data for inclusion verification is unlikely to be routine practice everywhere.

## What Cross-Referencing Could Reveal: Illustrative Evidence from Aadhaar

Where this kind of cross-referencing has occurred, even outside routine institutional practice, it illustrates the cost of the coordination gap. In December,2017, a study of Aadhaar-based biometric authentication in Andhra Pradesh's Public Distribution System (PDS) linked authentication failure logs with the state's beneficiary and ration card records, covering 3.77 million ration cards over a two-week period. It found a statewide authentication failure rate of 2.5 percent, with district-level rates in YSR Kadapa and Vizianagaram more than twice the state average. Biometric mismatch accounted for approximately 92 percent of all authentication failures (Singh & Chhatre, 2019). Because failure rates varied significantly across districts and were not simply proportional to the number of ration cards issued, the analysis pointed to localised causes of exclusion that a system-wide compliance or security metric alone would not have revealed.

A smaller case study of Mundoti, a village in Rajasthan's Ajmer district, based on interviews with 40 residents, similarly found that residents engaged in agricultural labour experienced disproportionately high rates of fingerprint-based authentication failure, and that age, gender, and occupation were associated with the likelihood of authentication problems (Jakhar, 2024). In that study, occupation was gathered through interviews rather than drawn from an official database field, since occupation is not part of the Aadhaar demographic record (Jakhar, 2024).

Both studies were conducted by outside researchers, not as part of a routine institutional audit or oversight process. That fact is itself evidence for this article's argument. The analytical potential of cross-referencing DPI operational and audit data with sectoral records is demonstrable, but realising it necessitates coordination mechanisms between disparate data systems.

## Towards Closing the Gap: Principles for Responsible Cross-Referencing

Closing this coordination gap requires more than technical interoperability; it requires a governance framework that treats the cross-referencing of audit data with sectoral administrative data as a deliberate, purpose-bound institutional function. Five principles should underpin such an approach.

- **Designated coordination mechanisms:** Routine cross-referencing should be supported by formal institutional arrangements—such as memoranda of understanding, inter-agency working groups, or dedicated coordination units—that connect supreme audit institutions, DPI regulators, and the sectoral ministries responsible for demographic and programme data (UN DESA, 2007).
- **Purpose limitation:** Any linkage between audit data and sectoral data should be tied to a defined, legitimate public-interest evaluation purpose, such as assessing inclusion or safety outcomes, and not repurposed for unrelated administrative, commercial, or enforcement uses General Data Protection Regulation (GDPR, 2021).
- **Privacy-preserving analytics:** Where individual-level linkage is necessary to detect exclusion patterns, findings should be reported through aggregation, de-identification, and other privacy-enhancing techniques that minimise re-identification risk, consistent with the Universal DPI Safeguards Framework's operational principles on privacy and security by design (UNDP & ODET, 2024).
- **Independent oversight:** Responsibility for authorising and reviewing cross-referencing exercises should sit with a body structurally separate from the entities being evaluated, consistent with the emphasis both INTOSAI and the UN DESA report place on audit independence as a precondition for credible, cross-cutting audit work (SAI Performance Measurement Framework [October 2025]; UN DESA, 2025).
- **Transparency:** Aggregate findings and the methodologies used to produce them should be published, so that the analytical value of cross-referenced audit data is available to policymakers and the public without requiring disclosure of individual-level records (UNDP, 2023).

## References

Art. 5 GDPR – Principles relating to processing of personal data - General Data Protection Regulation (GDPR). (2021, October 22). General Data Protection Regulation (GDPR). https://gdpr-info.eu/art-5-gdpr/

INTOSAI Development Initiative & INTOSAI Capacity Building Committee. (2025). Supreme Audit Institutions Performance Measurement Framework (SAI PMF), Version 2025. INTOSAI Development Initiative. https://idi.no/wp-content/uploads/2025/11/FINAL-2025-SAI-PMF.pdf

Jakhar, H. (2024). Unmasking Aadhaar authentication issues: A case study of biometric and PDS access in Mundoti, Rajasthan. Indian Journal of Social Science and Literature, 3(3), 28–32. https://doi.org/10.54105/ijssl.C1114.03030324

Muralidharan, K., Niehaus, P., & Sukhtankar, S. (2025). Identity verification standards in welfare programs: Experimental evidence from India. The Review of Economics and Statistics, 107(2), 372–392. https://doi.org/10.3386/w26744

OECD. (2019). The Path to Becoming a Data-Driven Public Sector (OECD Digital Government Studies). OECD Publishing. https://doi.org/10.1787/059814a7-en

OECD. (2026). Strengthening digital public infrastructure and data governance: Digital Government Outlook 2026. OECD Publishing.

https://www.oecd.org/en/publications/digital-government-outlook_0496b2bc-en/full-report/strengthening-digital-pu blic-infrastructure-and-data-governance_2c7323c7.html

Singh, S., & Chhatre, A. (2019). Aadhaar authentication failure in the public distribution system of Andhra Pradesh. ISB-Digital Identity Research Initiative.

https://www.isb.edu/faculty-and-research/research-directory/aadhaar-authentication-failure-in-the-public-distribution-system-of-andhra-pradesh

United Nations Department of Economic and Social Affairs. (2025). World Public Sector Report 2025: Supreme audit institutions and the Sustainable Development Goals. United Nations. https://desapublications.un.org/publications/world-public-sector-report-2025

Chapter Seven: Creating national institutions to implement and monitor the Convention – Coordination mechanisms

| United Nations Enable. (n.d.).

https://www.un.org/development/desa/disabilities/resources/handbook-for-parliamentarians-on-the-convention-on-the-rights-of-persons-with-disabilities/chapter-seven-creating-national-institutions-to-implement-and-monitor-the-con vention-2.html

United Nations Development Programme & UN Office for Digital and Emerging Technologies. (2024). Universal DPI Safeguards Framework. United Nations Development Programme. https://www.dpi-safeguards.org/framework

UNDP. (2023). The DPI Approach: A Playbook. In UNDP Publications. https://www.undp.org/publications/dpi-approach-playbook

# Auditing Digital Public Infrastructure for Inclusive Governance: Insights from India's Direct Benefit Transfer Experience

**Sameer Asif**
O/o the Comptroller & Auditor General of India



## Abstract

Digital Public Infrastructure (DPI) has emerged as a foundational component of modern governance by enabling governments to deliver public services through integrated digital identity, payment, and data-sharing systems. India's Digital Public Infrastructure, comprising Aadhaar, Jan Dhan bank accounts, the Unified Payments Interface (UPI), and the Direct Benefit Transfer (DBT) ecosystem, is widely recognised for improving financial inclusion and enhancing the efficiency of welfare delivery. At the same time, concerns relating to exclusion, privacy, data governance, technological resilience, and institutional accountability continue to shape policy debates. This article examines India's DBT ecosystem through the perspective of public sector auditing and proposes a practical framework for evaluating whether Digital Public Infrastructure promotes inclusive governance. The study adopts a qualitative and analytical approach based on a review of government reports, international policy documents, academic literature, and publicly available statistical data. It develops a five-dimensional audit framework focusing on access and inclusion, interoperability and traceability, privacy and data protection, resilience and continuity, and institutional governance and vendor management. The article argues that Supreme Audit Institutions should expand conventional financial and compliance audits to include broader assessments of equity, transparency, accountability, and citizen outcomes. By integrating principles of public value with performance auditing, the proposed framework provides a structured approach for evaluating whether Digital Public Infrastructure strengthens democratic governance while ensuring that technological innovation remains inclusive, accountable, and citizen-centered.

## Keywords

Digital Public Infrastructure, Inclusive Governance, Direct Benefit Transfer, Supreme Audit Institutions, Public Value, Performance Audit.

## Introduction

The rapid expansion of digital technologies has transformed the manner in which governments design, deliver, and monitor public services. Across the world, governments are increasingly investing in Digital Public Infrastructure (DPI) to strengthen administrative efficiency, improve financial inclusion, and expand access to essential public services. Unlike traditional e-government initiatives that focused on digitising individual departments, Digital Public Infrastructure provides common digital foundations—such as digital identity systems, interoperable payment platforms, and secure data exchange mechanisms—that enable multiple public and private services to operate on shared technological infrastructure.

India has emerged as one of the leading examples of Digital Public Infrastructure at scale. The country's digital ecosystem is built around the integration of Aadhaar as a digital identity platform, Jan Dhan accounts for financial inclusion, mobile connectivity, the Unified Payments Interface (UPI), and the Public Financial Management System (PFMS). Together, these systems support the Direct Benefit Transfer (DBT) programme, through which welfare benefits are transferred directly into beneficiaries' bank accounts. According to official government data, DBT has facilitated transfers amounting to several lakh crore rupees (approximately US$10 billion) while reducing delays and improving transparency in welfare administration. The rapid adoption of UPI and the expansion of financial inclusion further demonstrate the transformative potential of India's digital governance architecture.

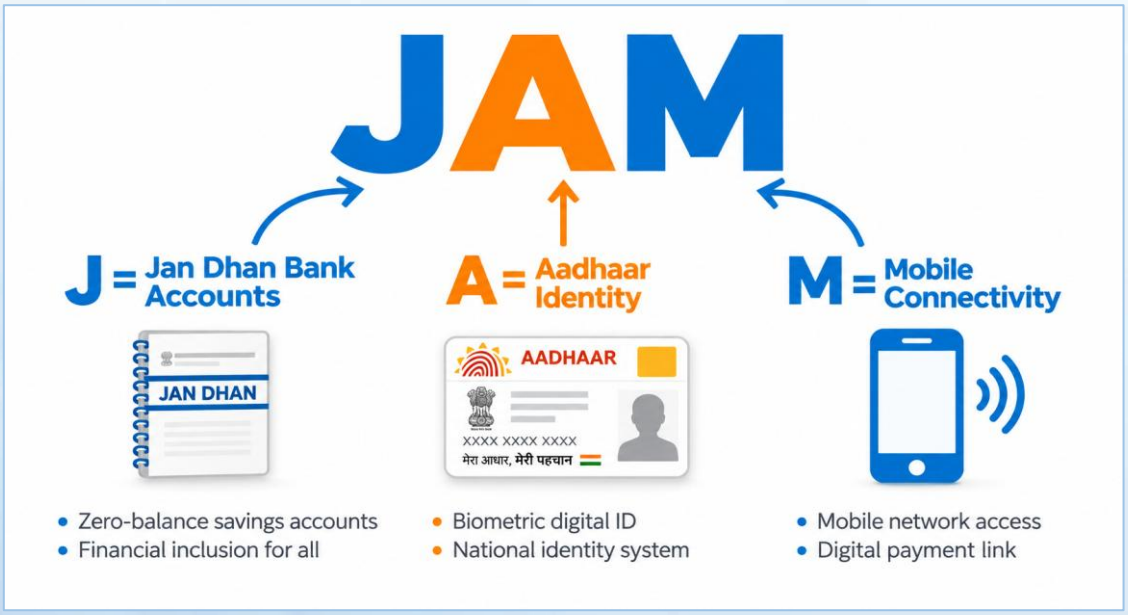



*Figure 1: India's JAM trinity.*

However, the success of Digital Public Infrastructure cannot be assessed solely through indicators such as transaction volumes, financial savings, or technological adoption. A growing body of academic research argues that digital systems may unintentionally reinforce existing inequalities when citizens experience barriers related to digital literacy, connectivity, biometric authentication failures, accessibility, or limited grievance redress mechanisms. Similarly, increasing dependence on integrated digital platforms raises important questions concerning data protection, cybersecurity, institutional accountability, and the role of private technology providers in delivering essential public services.

These competing perspectives indicate that evaluating Digital Public Infrastructure requires a broader understanding of public value. Efficient service delivery is an important objective, but governments must also ensure that digital systems remain accessible, transparent, equitable, resilient, and accountable. In this context, Supreme Audit Institutions (SAIs) play an increasingly significant role by examining whether investments in Digital Public Infrastructure achieve their intended public objectives while protecting citizens' rights and maintaining public trust.

Although several studies have examined India's Digital Public Infrastructure from technological, economic, and governance perspectives, relatively few have explored how Supreme Audit Institutions can systematically audit these complex digital ecosystems. Existing audit approaches often emphasise financial compliance or information technology controls without adequately assessing broader dimensions of inclusive governance. As governments continue expanding Digital Public Infrastructure into healthcare, education, taxation, agriculture, and social protection, there is a growing need for audit frameworks capable of evaluating both technical performance and societal outcomes.

This article addresses that gap by proposing a practical audit framework for assessing Digital Public Infrastructure through the lens of inclusive governance. Using India's Direct Benefit Transfer ecosystem as an illustrative case, the article identifies five interrelated dimensions that can guide public sector auditors: **(i) access and inclusion, (ii) interoperability and traceability, (iii) privacy and data protection, (iv) resilience and continuity, and (v) institutional governance and vendor management.** Rather than treating digital infrastructure as a purely technological investment, the proposed framework views it as public value infrastructure whose effectiveness should be measured by its contribution to equitable service delivery, transparency, accountability, and citizen welfare.

The findings of this study are intended to contribute to ongoing discussions on performance auditing, digital governance, and public administration by offering a practical framework that may assist Supreme Audit Institutions in evaluating Digital Public Infrastructure across different sectors and jurisdictions.

## Digital Public Infrastructure and Inclusive Governance: Concepts and Theories

Digital Public Infrastructure (DPI) refers to a set of foundational digital systems that enable governments, businesses, and citizens to access and deliver services efficiently through interoperable digital platforms. Unlike standalone e-governance initiatives that digitise individual public services, DPI establishes a common digital infrastructure that supports multiple applications across sectors. The G20 Task Force on Digital Public Infrastructure defines DPI as interoperable digital systems built on open standards that facilitate secure identity verification, digital payments, and trusted data exchange while encouraging innovation and public participation (India's G20 Task Force on Digital Public Infrastructure, 2024).

India's Digital Public Infrastructure has become one of the largest digital governance ecosystems globally. The integration of Aadhaar, Jan Dhan accounts, mobile connectivity, Unified Payments Interface (UPI), and the Public Financial Management System (PFMS) has transformed the delivery of welfare benefits, financial services, and public administration. The JAM (Jan Dhan–Aadhaar–Mobile) framework enables governments to identify beneficiaries, authenticate eligibility, and transfer financial assistance directly into bank accounts without multiple administrative intermediaries.

The rapid growth of India's digital ecosystem illustrates this transformation. More than 58 crore (580 million) Jan Dhan accounts have expanded financial inclusion, while Aadhaar has achieved near-universal coverage among residents. Similarly, UPI has emerged as one of the world's largest real-time payment systems, processing billions of transactions every month. These developments demonstrate how digital infrastructure can reduce transaction costs, improve transparency, and increase the efficiency of public expenditure.

However, technological expansion alone does not guarantee inclusive governance. Inclusive governance requires that digital systems remain accessible to all citizens irrespective of gender, income, literacy, disability, age, or geographical location. Public administration scholars increasingly argue that digital transformation should be evaluated not merely through technological adoption but through its ability to reduce inequality, strengthen accountability, and improve citizens' trust in public institutions (Mazzucato, Eaves, & Vasconcellos, 2024).

The concept of public value provides an important theoretical lens for understanding DPI. Public value extends beyond financial efficiency and considers whether government actions improve citizens' well-being, strengthen democratic institutions, and protect fundamental rights (Bozeman, 2007). From this perspective, Digital Public Infrastructure creates value only when it enables equitable access to public services while ensuring transparency, accountability, and protection of personal information.

Similarly, theories of inclusive governance emphasise participation, fairness, and equal access to opportunities. Digital platforms that exclude vulnerable populations because of poor connectivity, biometric failures, inaccessible interfaces, or weak grievance mechanisms may

inadvertently reinforce existing inequalities. Consequently, governments require evaluation mechanisms that measure not only technological performance but also social outcomes.

**Table 1: DPI components, inclusive governance goals, audit questions**

| DPI component | Example in India | Inclusive governance goal | Key audit questions |
|---|---|---|---|
| **Digital identity** | Aadhaar; e-KYC | Ensuring that every eligible person can be uniquely identified to access welfare schemes and rights. | • Are marginalised groups (rural poor, women, persons with disabilities) able to obtain Aadhaar and use it for services?<br>• How often does biometric authentication fail, and who is most affected? |
| **Payments rail** | UPI; PFMS; DBT | Delivering benefits directly to beneficiaries' accounts, reducing leakages and delays. | • Do DBT payments consistently reach the intended beneficiaries?<br>• What are the rates of failed or reversed transactions, and are they higher in particular regions or groups? |
| **Data-exchange layer** | IndiaStack APIs; DEPA data-sharing frameworks | Allowing secure, consent-based sharing of citizen data to access schemes and services. | • Is citizen data used only for clearly defined purposes?<br>• Are consent mechanisms understandable in practice (language, literacy, interface)? |

Supreme Audit Institutions (SAIs) therefore occupy an increasingly important position within digital governance. Traditionally responsible for examining financial compliance and public expenditure, SAIs are now expected to evaluate whether digital investments achieve intended policy objectives while safeguarding public resources and citizens' rights. Performance auditing of Digital Public Infrastructure must therefore combine financial accountability with broader assessments of inclusion, institutional effectiveness, and public value.

## India's DPI Ecosystem: Empirical Context

India's Direct Benefit Transfer (DBT) programme represents one of the most comprehensive applications of Digital Public Infrastructure in public administration. Introduced to improve welfare delivery, DBT seeks to transfer subsidies and social benefits directly into beneficiaries' bank accounts, thereby reducing administrative delays, leakages, and opportunities for corruption.

The programme integrates several components of India's digital ecosystem. Aadhaar enables unique identification of beneficiaries, Jan Dhan accounts facilitate financial inclusion, PFMS manages fund flows across government departments, and UPI provides a secure and interoperable payments infrastructure. Together, these systems enable government departments to deliver welfare benefits through an integrated digital architecture.

According to government estimates, DBT has facilitated direct transfers exceeding ₹49 lakh crore ($ 518.13 billion USD) while generating substantial savings through the elimination of duplicate or ineligible beneficiaries. The Expansion of Jan Dhan accounts and increased adoption of digital payment systems have also broadened access to formal financial services, particularly among economically weaker sections.

These achievements have strengthened the perception that Digital Public Infrastructure enhances state capacity by improving efficiency, reducing transaction costs, and increasing transparency. Digital records allow government agencies to monitor expenditure in real time, reconcile financial transactions, and identify irregularities more effectively than paper-based systems.

Despite these achievements, the DBT ecosystem has also attracted significant academic and policy debate. Several studies have documented challenges associated with biometric authentication failures, Aadhaar-bank account mismatches, inactive accounts, poor internet connectivity, and limited digital literacy. These issues disproportionately affect elderly citizens, migrant workers, persons with disabilities, and residents of remote rural areas who may already face barriers in accessing public services.

Another emerging concern relates to grievance redress mechanisms. While digital platforms automate benefit delivery, resolving errors often requires beneficiaries to interact with multiple agencies, banks, local officials, or service providers. Delays in correcting data mismatches or authentication failures may temporarily deprive eligible citizens of essential welfare benefits.

Privacy and data governance constitute another important area of concern. Digital welfare systems process sensitive personal information, including identity details, financial records, and socio-economic characteristics. Consequently, ensuring compliance with data protection principles, limiting unnecessary data sharing, and maintaining cybersecurity have become essential components of responsible digital governance.

The increasing participation of private technology firms, banking correspondents, payment service providers, and software vendors further complicates institutional accountability. While collaboration between government and private actors has accelerated technological innovation, it has also created new governance challenges regarding procurement, oversight, contractual accountability, and protection of citizens' interests.

These competing perspectives demonstrate that India's DBT ecosystem cannot be evaluated solely through financial savings or transaction volumes. Instead, it requires multidimensional

assessment capable of measuring efficiency alongside inclusion, resilience, accountability, and public trust. This provides the foundation for developing an audit framework that reflects the broader objectives of Digital Public Infrastructure.

**Table 2: Basic indicators of India's DPI/DBT ecosystem**

| Indicator | Value (with time period) | What it shows |
|---|---|---|
| **Total DBT transfers** | About ₹49.09 lakh crore ($512.76 billion USD) transferred up to early 2026. | Scale of direct transfers routed through DPI rails, showing how central DBT has become to welfare delivery. |
| **Claimed savings from DBT** | About ₹4.31 lakh crore ($45.08 billion USD) "saved" between 2015 and March 2024 by removing duplicate and fake beneficiaries. | Government's estimate of leakage reduction; a starting point for SAIs to test value-for-money and check how these savings are calculated. |
| **Number of Jan Dhan accounts** | Roughly 58 crore (580 million) accounts by 2026. | Expansion of basic bank accounts needed for DBT and financial inclusion. |
| **UPI transaction volume** | Around 21–22 billion transactions in January 2026, with extremely high total value. | Widespread use of the payments rail that underlies many DPI-enabled services. |

Against this background, India's Direct Benefit Transfer ecosystem is a particularly instructive domain for SAIs seeking to audit DPI's impact on inclusive governance.

## 4. A Five-Dimensional Audit Framework for Digital Public Infrastructure

The increasing adoption of Digital Public Infrastructure (DPI) requires Supreme Audit Institutions (SAIs) to move beyond traditional financial and compliance audits towards multidimensional assessments of governance outcomes. Conventional IT audits primarily focus on system security, procurement compliance, and financial accountability. While these remain important, they are insufficient for evaluating whether digital platforms actually improve public service delivery and strengthen inclusive governance. This article proposes a five-dimensional audit framework that combines principles of public value, digital governance, and performance auditing to evaluate the effectiveness of Digital Public Infrastructure.

### 4.1 Access and Inclusion

The first dimension examines whether Digital Public Infrastructure expands equitable access to public services for all sections of society. Inclusive governance requires governments to ensure that technological systems do not unintentionally exclude citizens because of income, age, disability, geography, gender, language, or digital literacy.

Within India's Direct Benefit Transfer (DBT) ecosystem, auditors should examine whether eligible beneficiaries are able to receive welfare benefits without unnecessary administrative barriers. Performance indicators may include Aadhaar coverage, Jan Dhan account utilisation, successful authentication rates, accessibility for persons with disabilities, multilingual service delivery, and the availability of alternative authentication mechanisms where biometric verification fails.

Field verification is particularly important because aggregate national statistics may conceal regional disparities. Audit teams should therefore combine administrative data with beneficiary interviews, local inspections, and grievance records to identify populations experiencing systematic exclusion. Such evidence enables auditors to distinguish between high overall coverage and genuinely inclusive service delivery.

## 4.2 Interoperability and Traceability

Digital Public Infrastructure derives much of its effectiveness from interoperability between different government databases and payment platforms. The integration of Aadhaar, PFMS, banking networks, UPI, and departmental databases enables information to move efficiently across institutions. However, interoperability must also be accompanied by comprehensive audit trails that allow every significant transaction to be reconstructed.

Auditors should assess whether common data standards are consistently applied across systems and whether each payment can be traced from budget allocation to final beneficiary. Complete transaction logs, reconciliation reports, and exception reports should be available to facilitate audit verification. Particular attention should be given to failed transactions, duplicate payments, and unexplained reversals, as these may indicate weaknesses in system design or operational controls.

Strong traceability enhances transparency, reduces opportunities for fraud, and strengthens institutional accountability by allowing auditors to identify where errors originate within the digital ecosystem.

## 4.3 Privacy and Data Protection

As governments increasingly rely on digital platforms, the collection and processing of personal information have become central governance issues. Digital identity systems, financial databases, and welfare records contain overly sensitive information that must be protected through appropriate legal, technical, and organisational safeguards.

An effective audit should therefore assess compliance with applicable data protection legislation and internationally recognised principles such as purpose limitation, data minimisation, secure storage, access control, and accountability. Auditors should verify whether personal information is collected only for legitimate public purposes, whether citizens receive meaningful information

regarding the use of their data, and whether adequate cybersecurity measures protect against unauthorised access or data breaches.

Where private technology vendors participate in processing government data, audit procedures should also examine contractual safeguards, responsibilities for incident reporting, and mechanisms for regulatory oversight. Public confidence in Digital Public Infrastructure depends not only on service efficiency but also on citizens' trust that their personal information will be handled responsibly.

## 4.4 Resilience and Continuity

Digital Public Infrastructure increasingly supports essential public services. Consequently, interruptions arising from cyberattacks, network failures, power outages, software defects, or natural disasters may directly affect citizens' access to welfare benefits and other government services.

Auditors should evaluate organisational resilience through reviews of disaster recovery plans, business continuity arrangements, backup infrastructure, cybersecurity incident reports, and recovery time objectives. Testing should also assess whether alternative service delivery mechanisms remain available during system failures, particularly for vulnerable populations living in areas with limited digital connectivity.

The resilience dimension extends beyond technical reliability. Service continuity should be assessed from the citizen's perspective by considering whether individuals experience delays, repeated travel, or additional financial costs when digital systems become unavailable. Such impacts are particularly significant for beneficiaries who depend on government assistance for their livelihoods.

## 4.5 Institutional Governance and Vendor Management

The final dimension recognises that Digital Public Infrastructure operates within complex institutional arrangements involving multiple government agencies, regulators, financial institutions, technology providers, and service vendors. Effective governance requires clearly defined responsibilities, transparent procurement practices, independent oversight, and robust accountability mechanisms.

Audit teams should review governance structures, contractual arrangements, procurement procedures, performance indicators, conflict-of-interest safeguards, and mechanisms for monitoring vendor performance. Particular attention should be paid to concentration risks where essential digital services depend heavily upon a limited number of private providers.

Institutional governance should also examine coordination among participating agencies. Weak communication, overlapping responsibilities, or fragmented accountability may reduce

operational effectiveness even where technological systems perform satisfactorily. Consequently, governance audits should evaluate both organisational capacity and institutional collaboration across the Digital Public Infrastructure ecosystem.

**Table 3: Five-dimensional audit framework**

| Dimension | What it means | What auditors should look at |
|---|---|---|
| **Access and inclusion** | Whether DPI actually helps more people, especially those at the margins, to receive benefits and exercise rights. | • Coverage of Aadhaar, bank accounts, mobile connectivity by gender, region, social group.<br>• Places where people are failing to get benefits (e.g., biometric failures, inactive accounts, language barriers).<br>• Grievance data and field observations. |
| **Interoperability and traceability** | Whether systems (PFMS, banks, scheme databases, Aadhaar) work together smoothly and keep clear records. | • Consistent identifiers across systems.<br>• Complete transaction logs that show the full path of a payment.<br>• Reconciliation reports and how error codes are recorded and analysed. |
| **Privacy and data protection** | Whether DPI respects data-protection principles and gives citizens meaningful control over their data. | • Policies and laws on data use and retention.<br>• How consent is collected and presented to users.<br>• Agreements with private vendors on data sharing and safeguards. |
| **Resilience and continuity** | Whether DPI continues to work during outages, attacks, or disasters, especially for those who depend on it most. | • Disaster-recovery and backup plans.<br>• Records of outages and where they hit hardest.<br>• Availability of alternative delivery modes if online systems fail. |
| **Institutional governance and vendor management** | Who controls and oversees DPI, and how public and private actors are held accountable. | • Mandates and roles of DPI bodies and regulators.<br>• Procurement and contract documents for core DPI systems.<br>• Market concentration among vendors; oversight by regulators, parliaments, and SAIs. |

## 5. Discussion

The proposed framework demonstrates that evaluating Digital Public Infrastructure requires a broader perspective than conventional assessments of financial savings or technological

efficiency. India's experience illustrates that digital systems can significantly improve welfare delivery while simultaneously creating new governance challenges relating to inclusion, privacy, cybersecurity, and institutional accountability.

For Supreme Audit Institutions, this implies expanding performance audit methodologies to include both quantitative and qualitative evidence. Administrative data should be complemented by field observations, beneficiary surveys, stakeholder consultations, and analysis of grievance records. Such an integrated approach enables auditors to identify whether observed improvements in efficiency are accompanied by equitable service delivery across different social and geographical groups.

The framework also encourages greater collaboration between financial auditors, information technology specialists, cybersecurity professionals, and public policy experts. As governments continue investing in Digital Public Infrastructure across sectors such as healthcare, education, agriculture, taxation, and social protection, multidisciplinary audit teams will become increasingly necessary.

Although this study focuses on India's Direct Benefit Transfer ecosystem, the proposed framework has broader relevance. Many countries are currently developing digital identity systems, interoperable payment platforms, and integrated government databases. The audit principles proposed here may therefore assist Supreme Audit Institutions in adapting existing performance audit methodologies to emerging digital governance environments while remaining sensitive to national legal and institutional contexts.

## 6. Conclusion

Digital Public Infrastructure has fundamentally transformed the delivery of public services by integrating digital identity, payment systems, and interoperable data platforms. India's Direct Benefit Transfer ecosystem demonstrates both the opportunities and the challenges associated with large-scale digital governance. While Digital Public Infrastructure has strengthened financial inclusion, increased administrative efficiency, and improved transparency in welfare delivery, its long-term success ultimately depends on ensuring equitable access, protecting citizens' rights, maintaining operational resilience, and strengthening institutional accountability.

This article has proposed a five-dimensional audit framework comprising access and inclusion, interoperability and traceability, privacy and data protection, resilience and continuity, and institutional governance and vendor management. Together, these dimensions provide Supreme Audit Institutions with a practical framework for evaluating whether Digital Public Infrastructure creates sustainable public value rather than merely digitising administrative processes.

Future research may apply and validate this framework through empirical audits of specific welfare programmes, comparative international studies, or quantitative assessments of audit outcomes. As digital transformation continues to reshape public administration worldwide,

independent auditing will remain essential to ensuring that technological innovation supports democratic governance, transparency, and inclusive development.

## References


- Alonso, C., et al. (2023). *Stacking up the benefits: Lessons from India's digital journey* (IMF Working Paper 2023/078). International Monetary Fund.
- Bozeman, B. (2007). *Public Values and Public Interest*. Georgetown University Press.
- DEF India et al. (2023). *A Governance Framework for Digital Public Infrastructure: Learning from the Indian Experience*. T20 Policy Brief.
- India's G20 Task Force on Digital Public Infrastructure. (2024). *Report of India's G20 Task Force on Digital Public Infrastructure*. Government of India.
- IT for Change. (2025). *Recovering the "Public" in India's Digital Public Infrastructure Strategy*. Policy Brief.
- Mazzucato, M., Eaves, D., & Vasconcellos, B. (2024). *Digital Public Infrastructure and Public Value: What is "Public" About DPI?* UCL Institute for Innovation and Public Purpose.



Section V

# THE AUDIT RESPONSE: FRAMEWORKS, GUIDELINES AND FIELD EXPERIENCE

The professional core, in two movements.



Section V(A)

# FRAMEWORKS AND GUIDELINES

# Auditing Decision Accountability in AI-Enabled DPI: Lessons from a Social Impact Study of Welfare Schemes in India

**Bijay Kumar Mohanty**
Additional Deputy Comptroller & Auditor General, India





**Krishnan Narayanan**
Co-founder and President, itihaasa Research and Digital



**V.R. Muraleedharan**
Professor Emeritus, Department of Humanities and Social Sciences, IIT Madras

## Abstract

Governments are entering a co-intelligence era in which public decisions are increasingly shaped by human judgement, data systems, artificial intelligence, and societal systems working together. Digital Public Infrastructures (DPIs) have already changed the scale and speed of public service delivery through shared rails for identity, payments, document exchange, data flows, and welfare access. As these infrastructures become AI-enabled, public audit faces a new assurance challenge. It must examine whether digitally mediated decisions are explainable, verifiable, appealable, and aligned with inclusive governance.

Drawing on a primary social impact review of welfare schemes by the office of the Comptroller and Auditor General (C&AG) of India, we argue that the next frontier of welfare audit is decision accountability. The study covered eight major welfare and entitlement schemes across seven

Indian states and combined scheme database analytics, household surveys, and field verification. Its detailed findings remain unpublished; we therefore use the study mainly to derive qualitative audit lessons. The review indicated substantial welfare reach, while also surfacing recurring challenges around fragmented records, stale data, last-mile delivery gaps, weak grievance linkage, and limited household-level visibility across schemes.

We propose a co-intelligence audit architecture: common decision language, authoritative facts, published rules, decision traces, data provenance, citizen-facing appeal records, privacy-preserving audit access, and AI-supported audit assertions under human supervision. Within AI-enabled DPI, every material welfare decision should be able to explain itself, prove its integrity, be tested by audit, and be challenged by the citizen.

## Keywords

Digital Public Infrastructure (DPI); Co-Intelligence; Public Audit; AI Governance; Decision Accountability; Welfare Delivery

## 1. Introduction: The shift from digital delivery to co-intelligence governance

Public administration is moving from a digital era to a co-intelligence era (Ramaswamy and Narayanan, 2025). Earlier waves of digital government focused on computerising records, automating workflows, and creating online service portals. The emerging phase is more complex. Public decisions now arise through interactions among citizens and communities, officials, databases, algorithms, AI-enabled tools, and institutional rules.

Digital Public Infrastructure (DPI) is central to this shift. The G20 defines DPI as shared digital systems that are secure and interoperable, may be built on open standards, and can support the inclusive delivery of public and private services at societal scale (G20 Digital Economy Working Group, 2023). Indian DPI has matured into a population-scale ecosystem for identity, payments, document exchange, and welfare delivery. Driven by high-volume systems like Aadhaar, Direct Benefit Transfer (DBT), and Unified Payments Interface (UPI), this network now provides a robust foundation for advanced AI-enabled capabilities, including beneficiary identification, fraud analytics, grievance classification, and decision support (Unique Identification Authority of India, n.d.; Direct Benefit Transfer Mission, n.d.; National Payments Corporation of India, n.d.).

As DPI evolves from supporting transactions and record-keeping to informing or shaping administrative decisions, the scope of audit must expand with it. Traditional IT controls remain essential for assessing issues such as system integrity, security, access, availability, and processing reliability. But they do not by themselves establish whether a welfare decision was substantively justified. A system may correctly record that a person was accepted, rejected, paid, excluded, verified, or flagged. However, it may leave unanswered why that outcome occurred,

whether the underlying facts were current and accurate, whether the correct rule was applied, who was accountable for the decision, and whether the citizen could effectively challenge it.

*Audit must therefore move beyond assuring the functioning of the technology to assuring the accountability of the decisions produced through it*.

## 2. Literature review: DPI, co-intelligence, commons governance, and public audit

The DPI literature marks a shift from isolated e-governance systems to reusable public infrastructure: shared rails for delivering services, exchanging trusted information, and building new applications, rather than fragmented departmental portals and scheme databases.

The World Bank stresses that DPI is an approach to digitalisation, not a single technology product, with value depending on governance, safeguards, public purpose, and ecosystem design (World Bank, 2025). Mazzucato et al. (2026) sharpen this: public value cannot be inferred from DPI's technical attributes or even its public provision alone, but depends on the direction, governance and process behind value creation — directly supporting this article's claim that audit must examine the accountability of decisions, not merely the functioning of systems.

UNDP's work connects DPI with development outcomes, noting reduction in transaction costs, access, trust, and innovation where risks are addressed through safeguards (United Nations Development Programme, 2023). The Universal DPI Safeguards Framework emphasises public interest, inclusion, equity, safety, trust, transparency, and accountability across the DPI lifecycle (Universal DPI Safeguards Initiative, 2024).

The co-intelligence (COIN) DPI perspective builds on this foundation. Ramaswamy and Narayanan (2025) frame co-intelligence as an emerging mode of value creation where humans and AI generate a new capability together, rather than AI functioning as a stand-alone automation tool. Ramaswamy et al. (2026) extend this to public infrastructure: DPIs can evolve from systems of record into systems of learning, where citizen interactions, institutional feedback, and AI-supported sensemaking improve governance over time.

Ostrom's work on social-ecological systems strengthens this argument: complex governance systems depend on feedback, contextual knowledge, and adaptive processes (Ostrom, 2009). Balabanova et al. (2011) add an institutional perspective, identifying four recurring conditions for sustained health-system reform: capacity, continuity, context, and catalysts. Together, these suggest that accountable infrastructures require not just technical architecture but feedback mechanisms and institutional capabilities that let systems learn and adapt.

Delivery-system literature adds a lifecycle perspective: Lindert et al. (2020) conceptualise social protection delivery as a journey from outreach and eligibility assessment through enrolment, benefit provision, monitoring, and grievance redress. This is particularly relevant to welfare DPIs,

where accountability must extend across the full beneficiary journey rather than individual transactions or scheme databases.

Audit and AI governance frameworks likewise broaden assurance beyond technical controls. ISSAI 3000 frames performance audit around economy, efficiency, and effectiveness, linked to accountability, transparency, and good governance (INTOSAI, 2019), while the WGITA-IDI Handbook recognises IT audit as central for Supreme Audit Institutions (SAIs) given government's growing dependence on information systems (INTOSAI Working Group on IT Audit, & INTOSAI Development Initiative, 2022). In India, the CAG's Artificial Intelligence Strategy Framework addresses AI use across the audit lifecycle and the capacity to audit AI systems (Comptroller and Auditor General of India, 2025). GAO's AI Accountability Framework calls for governance of data and performance alongside ongoing monitoring (Government Accountability Office, 2021), while NIST's AI Risk Management Framework treats trustworthy AI as a matter of governance, transparency, accountability, privacy, and fairness, not technical accuracy alone (National Institute of Standards and Technology, 2023).

Together, these sources suggest a practical conclusion: *AI-enabled DPIs should be audited as public decision ecosystems, not merely as technology platforms*.

## 3. The audit problem in AI-enabled welfare systems

Consider the following illustrative case, which shows how a single adverse outcome can emerge from failures across multiple systems, agencies, and decision rules. See Box 1.

*Box 1: An Illustrative Welfare Decision*

A citizen's welfare benefit is suddenly stopped. The system records only that she is no longer eligible. Yet the cause may lie anywhere in the decision chain: an outdated household record, failed authentication, incorrect bank seeding, incomplete field verification, or a mismatch in another departmental database. A duplicate flag may indicate fraud, but it could equally reflect migration, clerical error, or stale data. The citizen sees a single adverse outcome; the decision behind it may span multiple systems, agencies, and rule sets.

The case illustrates a central audit problem in welfare DPI. Relevant information – identity, household composition, bank validation, payment status, landholding, work demand, ration eligibility, health entitlement, asset verification, and grievances – may reside in separate repositories maintained by different agencies and updated at different intervals. Unless the decision can be reconstructed across these systems, audit cannot reliably determine whether an exclusion was legitimate or the result of administrative error.

Conventional audit remains essential: compliance, financial propriety, cybersecurity, internal controls, and system availability still matter. But these tests cannot fully establish whether a

citizen was fairly included or excluded. This is where *decision accountability* becomes critical: audit must be able to determine not just that a decision was recorded, but why it was made, on what basis, and whether the citizen had any means of challenging it.

## 4. Learnings from a primary social impact review of welfare schemes

The authors were part of the core team for a recent primary study conducted by the office of the Comptroller and Auditor General of India, which examined the social impact of major welfare and entitlement schemes across multiple Indian states. As the full findings remain unpublished, we draw upon this study cautiously, focusing on systemic design lessons rather than presenting detailed empirical results.

Two high-level data points establish the scale and relevance of the exercise. First, the review covered eight flagship welfare and entitlement schemes across seven states, combining scheme database analytics, household surveys, and field verification. Second, the data analytics examined approximately 12.7 million Antyodaya Anna Yojana (AAY) households (representing the poorest tier of beneficiaries), while the field component surveyed approximately 219,000 ration-card households. This scale was broad enough to surface recurring, structural audit questions across diverse schemes and geographies.

Our focus here is on the qualitative lessons. The study indicated substantial welfare reach, but also growing audit challenges as schemes and delivery systems become more interconnected. A household may receive multiple benefits, yet no single auditable view captures its complete entitlement lifecycle – from initial eligibility and application through to sanction, last-mile delivery, payment failure, and final grievance redressal.

The study also highlighted the limitations of scheme-centric administration. Departments traditionally view citizens through the narrow lens of their respective programmes. In contrast, citizens navigate welfare as a combined journey across food security, employment, health, housing, pensions, and agricultural support. The field review surfaced five recurring audit risks, summarised in Figure 1.

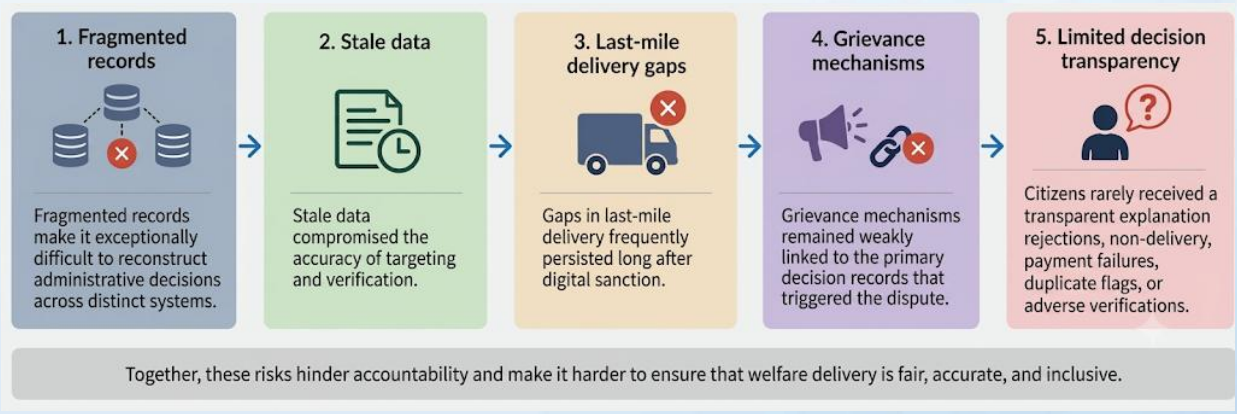



*Figure 1: Recurring Audit Risks Observed in Welfare Delivery*

## 5. From findings to audit architecture

One overarching lesson from the study is architectural: *welfare systems have significantly improved their ability to record events, but they still lack the structural capacity to explain decisions*. It suggests that the future of welfare audit should be built around *decision traceability*. See Figure 2.

The aim is not to create one master beneficiary database. Centralising records may increase privacy risk and can propagate errors when underlying data are stale, incomplete, or incorrectly matched. We therefore propose a *model of federated accountability*: responsible agencies retain and maintain authoritative facts, while common standards, provenance mechanisms, and authorised audit access allow decisions to be reconstructed and tested across systems.

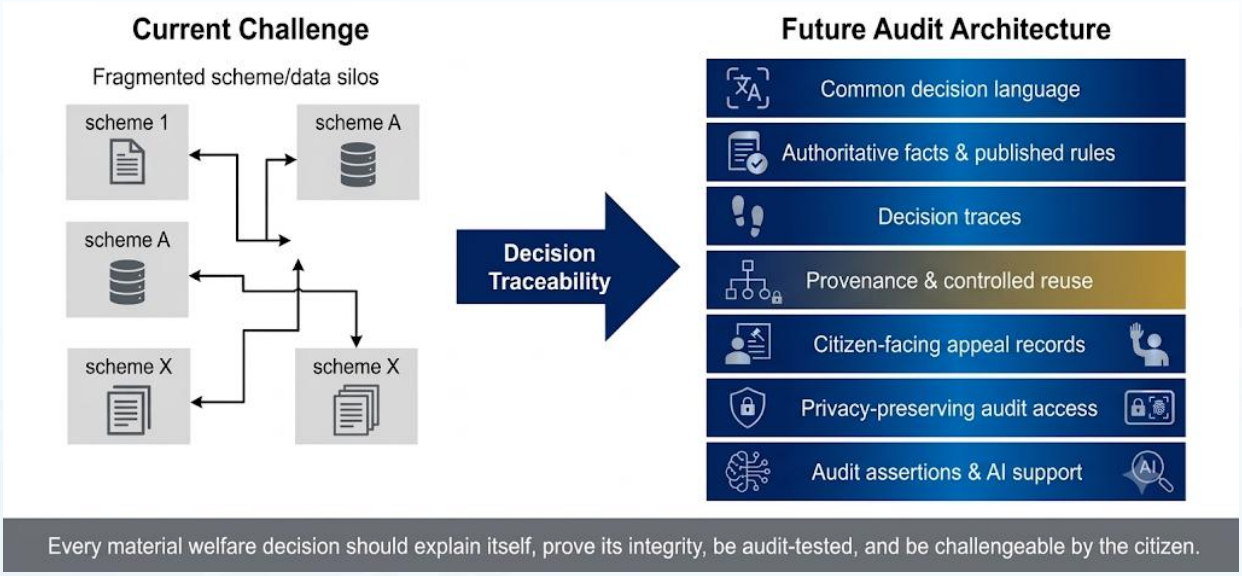



*Figure 2: Future Audit Architecture*

### 5.1 Common decision language

In the illustrative case (refer to Box 1), one system may record a failed authentication, another a change in household status, and a third simply record that the benefit was stopped. Unless these events use a common administrative vocabulary, reconstructing the decision becomes difficult.

Every material welfare event should therefore capture a minimum common set of elements: decision, rule, fact, source, evidence, authority, outcome, reason, time, and remedy. The same structure should apply across application, approval, rejection, payment, delivery, verification, grievance, and appeal. A common decision language does not require agencies to use a common database. It allows events recorded in different systems to be interpreted consistently, compared across schemes and tested by auditors. It also creates a structured basis for AI-supported anomaly detection and process testing.

## 5.2 Authoritative facts and published rules

Suppose the citizen's benefit was stopped because her household composition had changed. Audit must be able to establish which record supplied that fact, when it was last updated, and whether that source was authorised to determine it. If the outcome arose from a duplicate-detection or eligibility rule, the auditor must also know exactly which version of that rule was applied.

Material welfare facts, such as household composition, mortality, migration, disability status, landholding or bank credentials, should therefore map to designated authoritative sources with defined update responsibilities. Eligibility criteria, rejection conditions, duplicate-detection protocols and verification rules should likewise be versioned and available in human-readable and machine-executable form. This *separation of fact, rule and decision* makes it possible to determine whether an adverse outcome arose from valid ineligibility, inaccurate data or incorrect application of a rule.

## 5.3 Decision traces

Knowing the final outcome is not enough. A record stating that the citizen was "ineligible" does not explain how that conclusion was reached.

Every material decision should therefore leave a trace that records the rule invoked, facts and evidence used, source systems consulted, responsible authority, time of decision and available remedy. The distinction is important: an ordinary audit trail establishes what happened; *a decision trace helps establish why it happened*.

## 5.4 Provenance and controlled reuse

The citizen should also not be required to repeatedly prove the same fact to different agencies. If a competent authority has already verified a material fact, another authorised agency should be able to rely on it while retaining information about its source, date and validation history.

Such reuse must therefore carry *provenance*. An auditor should be able to determine where a reused fact originated, who validated it and whether it remained valid when the subsequent decision was made. Importantly, the absence of a reusable record should trigger further verification; not automatic denial of a benefit.

## 5.5 Citizen-facing appeal records

Decision accountability must also work from the citizen's side. In the illustrative case, being told simply that a benefit has stopped is insufficient. Every adverse decision should therefore

generate an intelligible explanation stating the reason, relevant rule, material facts relied upon, responsible agency, and route for correction or appeal.

This turns the decision trace from an internal audit artefact into a mechanism of *citizen accountability*. It also allows grievance and appeal outcomes to be linked back to the original decision rather than existing in a separate administrative silo.

### 5.6 Privacy-preserving audit access

Making the citizen's decision auditable does not require all underlying personal data to be pooled in one location. The identity agency, bank, welfare department or local administration may continue to retain the records for which each is responsible. Auditors should instead be able to execute authorised queries across those systems and receive only what is necessary for the audit purpose – for example, exception counts, trace references, anonymised samples or aggregated results.

The principle is therefore *federated auditability rather than centralised data accumulation*: reconstruct the decision across systems without unnecessarily replicating the citizen's underlying personal data.

### 5.7 Audit assertions and AI support

Once decisions are represented in this structured form, many basic accountability requirements can be expressed as reusable audit assertions. For example, "no rejection without a valid reason code," or "no delivery claims without verifiable evidence of receipt," among others of this kind. Applied to the illustrative citizen, such assertions could help identify whether her benefit was stopped without an authorised rule, on the basis of stale data, or without an accessible remedy.

AI can assist by running these tests across large datasets, identifying unusual patterns, prioritising cases for field verification and synthesising complex decision traces. But it does not determine whether an exclusion was ultimately justified. *That judgement remains with the auditor*, who must interpret evidence in its legal, administrative, and human context.

## 6. Implications for Supreme Audit Institutions

SAIs require a paradigm shift in *institutional capability* to remain effective in the co-intelligence era. While financial, compliance, performance, and IT audits remain indispensable core disciplines, they must be fundamentally reinforced with advanced competencies in data engineering, algorithmic AI governance, privacy-preserving analytics, and macro-systems thinking. Furthermore, SAIs must build capabilities in user-experience diagnostics and automated decision-trace testing to audit modern, interconnected public delivery networks.

SAI India (C&AG) has already begun building in this direction. In August 2026, CAG and Indian Institute of Technology (IIT) Madras launched a three-tier Certification on Audit of Digital Systems (CADS), covering public audit, IT, cybersecurity, information systems, digital public platforms, and AI. (Indian Institute of Technology Madras, 2026). It builds on an earlier IIT Madras programme whose graduates are already applying these skills in field audits. One further institutional response would be to extend this trajectory into a standing *Audit Assurance Lab*: a specialised, multidisciplinary unit that develops and maintains libraries of reusable automated audit assertions, evaluates high-risk algorithmic models in isolated sandboxes, runs algorithmic red-team exercises to stress-test systems for drift or systemic exclusion, and replicates automated rule logic through parallel testing environments to verify administrative fidelity.

Building such capability is not only a technical challenge but an institutional one – CADS's shift from a standalone cohort into a three-tier certification track suggests SAI India is already building the *continuity* that Balabanova et al.'s (2011) 4C lens identifies as necessary for capacity to become institutional rather than project-based. This evolution extends the traditional performance audit mandate towards a continuous, data-driven, and system-oriented model.

Crucially, *materiality itself must undergo a human-centric recalibration*. See Figure 3. In a scaled DPI, a seemingly negligible error rate, for example, in automated identity matching, can obscure catastrophic systemic exclusions when concentrated within highly vulnerable populations. A minor data mismatch ceases to be a trivial clerical discrepancy when it arbitrarily denies an eligible household access to food, medical care, employment, housing, or income support. SAIs should flag error rates concentrated among vulnerable beneficiary categories as material, regardless of aggregate value against conventional monetary thresholds.

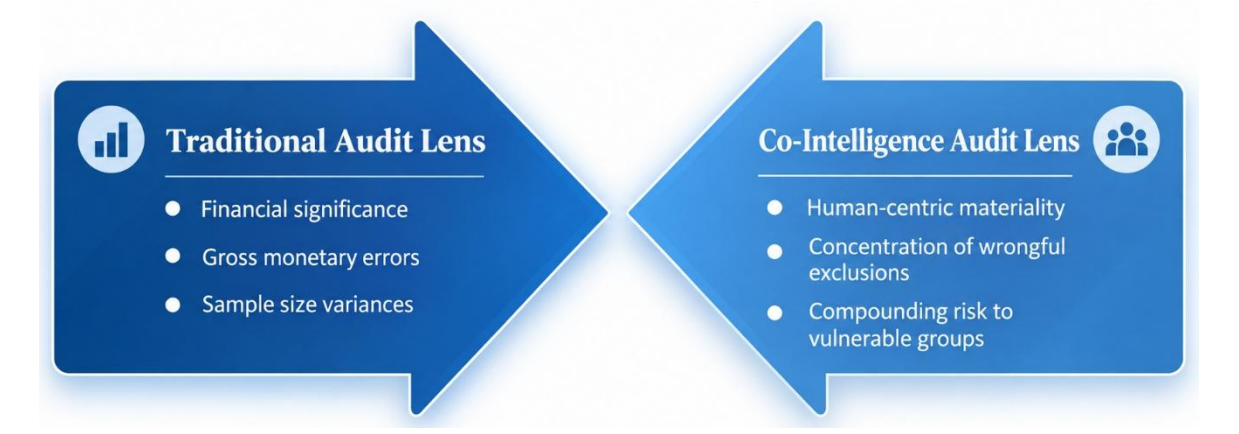



*Figure 3: Shifting the Audit Paradigm*

To operationalise this perspective, citizen feedback loops must be integrated into core audit intelligence. The primary study itself illustrates this: a one-off survey of ration-card households already surfaced evidence no scheme database could have captured. More systematically, anonymised grievance registries, field observations, and citizen-experience documentation can surface early warning signals of system breakdown that administrative databases miss.

Synthesised responsibly, these signals let auditors pinpoint algorithmic exclusion, bureaucratic delay, and grievance-remediation failure before they scale – making audit adaptive rather than merely retrospective, and feeding both corrective action and system redesign (Ostrom, 2009).

## 7. Conclusion

AI-enabled DPIs can expand the reach and responsiveness of welfare delivery. Their enduring public value, however, hinges on accountability at the exact point where citizens encounter the state: the administrative decision. Recording that a decision was made is not the same as explaining it: audit must examine the accountability of decisions, not merely the functioning of systems.

The primary study indicated substantial welfare reach, while surfacing recurring risks – fragmented records, stale data, last-mile delivery gaps, weak grievance linkage, and limited decision transparency – that isolated, scheme-centric databases are structurally unable to resolve. The federated model set out above responds to this directly: responsible agencies retain authoritative facts while common standards, decision traces, and provenance allow decisions to be reconstructed and tested across systems, without the privacy and error-propagation costs of full centralisation.

Realising this architecture is an institutional undertaking, not only a technical one. SAI India's own recent steps suggest this shift is already underway, from the CAG-IIT Madras Certification on Audit of Digital Systems to the primary review's own household survey, which shows that citizen feedback can surface what scheme databases alone cannot. What remains is to make such practices systematic rather than occasional.

This architecture is not self-executing, and its limits deserve acknowledgment alongside its case. Common decision language and provenance standards depend on many legacy-bound agencies adopting shared conventions – a political and administrative undertaking this paper has not resolved. The institutional capability that sustains it, of the kind CADS illustrates, presumes resources that not every SAI can command. And an audit apparatus built substantially around AI-assisted testing carries its own resource and ecological costs, which this paper has not examined.

Every material welfare decision should be able to explain itself, prove its integrity, be tested by audit, and be challenged by the citizen. As DPIs scale, public accountability must scale with them.

## Acknowledgements

The authors thank Manish Srivastava, CEO, AI CoE for Sustainable Cities, IIT Kanpur, for his review of the audit architecture and helpful suggestions.

## References

Balabanova, D., McKee, M., & Mills, A. (Eds.). (2011). *Good health at low cost 25 years on: What makes a successful health system?* London School of Hygiene & Tropical Medicine.

Comptroller and Auditor General of India. (2025). *Artificial intelligence strategy framework*. Supreme Audit Institution of India.

Direct Benefit Transfer Mission. (n.d.). *Direct Benefit Transfer Bharat dashboard*. Government of India. https://dbtbharat.gov.in/

G20 Digital Economy Working Group. (2023). *G20 framework for systems of digital public infrastructure*. G20 India Presidency.

Government Accountability Office. (2021). *Artificial intelligence: An accountability framework for federal agencies and other entities* (GAO-21-519SP). https://www.gao.gov/products/gao-21-519sp.

Indian Institute of Technology Madras. (2026, August 27). *CAG and IIT Madras Launch Certification on Audit of Digital Systems (CADS)* [Press release]. https://www.iitm.ac.in/happenings/press-releases-and-coverages/cag-and-iit-madras-launch-certification-audit-digital.

INTOSAI. (2019). *ISSAI 3000: Performance audit standard*. International Organization of Supreme Audit Institutions. https://www.issai.org/pronouncements/issai-3000-performance-audit-standard/.

INTOSAI Working Group on IT Audit, & INTOSAI Development Initiative. (2022). *WGITA-IDI handbook on IT audit for Supreme Audit Institutions*. https://idi.no/our-work/initiative/wgita-idi-handbook-on-it-audit/.

Lindert, K., Karippacheril, T. G., Rodríguez Caillava, I., & Nishikawa Chávez, K. (Eds.). (2020). *Sourcebook on the foundations of social protection delivery systems*. World Bank. https://doi.org/10.1596/978-1-4648-1577-5

Mazzucato, M., Eaves, D., & Vasconcellos, B. (2026). Digital public infrastructure and the economics of public value: what is 'public' about DPI? *Journal of Economic Policy Reform*, *29*(2), 113-141. https://doi.org/10.1080/17487870.2026.2662285

National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). U.S. Department of Commerce. DOI: https://doi.org/10.6028/NIST.AI.100-1

National Payments Corporation of India. (n.d.). *Unified Payments Interface: Product statistics*. https://www.npci.org.in/product/upi/product-statistics.

Ostrom, E. (2009). A general framework for analyzing sustainability of social-ecological systems. *Science, 325*(5939), 419–422. DOI: https://doi.org/10.1126/science.1172133

Ramaswamy, V., & Narayanan, K. (2025). *The co-intelligence revolution: How humans and AI co-create new value*. Penguin Business.

Ramaswamy, V., Özcan, K., & Narayanan, K. (2026). *Co-creating the future with AI*. Palgrave Macmillan.

Unique Identification Authority of India. (n.d.). *Aadhaar dashboard*. Government of India. https://uidai.gov.in/aadhaar_dashboard/.

United Nations Development Programme. (2023). *Accelerating the SDGs through digital public infrastructure: A compendium of the potential of digital public infrastructure*. UNDP. https://www.undp.org/publications/accelerating-sdgs-through-digital-public-infrastructure-compendium-potential-digital-public-infrastructure.

Universal DPI Safeguards Initiative. (2024). *Universal DPI safeguards framework: A guide to building safe and inclusive digital public infrastructure for societies*. https://www.dpi-safeguards.org/.

World Bank. (2025). *Digital public infrastructure and development: A World Bank Group approach*. World Bank Group. http://documents.worldbank.org/curated/en/099031025172027713.

# Auditing Digital Public Infrastructure: Strengthening Inclusive Governance through Supreme Audit Institutions



**Serah Kituu**
Office of the Auditor-General, Kenya

## Abstract

Digital Public Infrastructure (DPI) has become a strategic enabler of public administration by supporting digital identity, electronic payments, data exchange, revenue collection, and integrated public service delivery. In Kenya, platforms such as eCitizen, the Integrated Financial Management Information System (IFMIS), digital identity systems, and the Social Health Authority (SHA) have transformed the delivery of government services by enhancing efficiency, accessibility, and transparency. However, the increasing reliance on interconnected digital platforms also introduces significant governance, financial, operational, cybersecurity, privacy, and service continuity risks that may adversely affect public accountability and citizen trust.

This paper examines the role of Supreme Audit Institutions (SAIs) in providing independent assurance over Digital Public Infrastructure through a risk-based audit approach. Using a documentary review and analytical synthesis of Kenyan legislation, public policies, audit reports, regulatory guidance, and the International Standards of Supreme Audit Institutions (ISSAIs), the study develops a comprehensive assurance framework for auditing DPI as a public governance ecosystem rather than a standalone technology initiative.

The analysis identifies six critical audit domains requiring assurance: governance and institutional arrangements; inclusion and accessibility; identity and eligibility controls; data governance and privacy; interoperability and data quality; and financial integrity, cybersecurity, and operational resilience. The paper argues that, because DPI simultaneously affects public finances, service delivery, citizens' rights, and institutional trust, effective oversight requires an integrated application of financial, compliance, performance, and information systems auditing.

The study concludes that auditing Digital Public Infrastructure should extend beyond evaluating system functionality to assessing whether digital platforms operate in accordance with applicable legal and regulatory frameworks, safeguard public resources, protect personal data, promote equitable access to public services, and deliver sustainable public value. By adopting a risk-based and multidisciplinary audit approach, Supreme Audit Institutions can strengthen accountability, enhance transparency, improve governance, and reinforce public confidence in digital government.

## Keywords

Digital Public Infrastructure (DPI), Supreme Audit Institutions, Inclusive Governance, Public Accountability, Risk-Based Auditing, Digital Government.

## 1. Introduction

Digital Public Infrastructure (DPI) has emerged as a critical enabler of state capacity and public sector transformation. The World Bank defines DPI as foundational digital building blocks designed for public benefit, while the United Nations Development Programme (UNDP) emphasizes open, interoperable, and inclusive digital systems governed through transparent and accountable institutional frameworks (UNDP, 2023; World Bank, 2025). Collectively, these perspectives position DPI not as individual digital applications but as shared public infrastructure that underpins the delivery of multiple government services.

Kenya has made significant progress in implementing Digital Public Infrastructure (DPI). The eCitizen platform serves as a single gateway to government services, supported by the Kenya National Digital Master Plan 2022–2032 and Executive Order No. 2 of 2023, which strengthen integrated digital service delivery and digital governance.

As governments increasingly rely on shared digital platforms, weaknesses in one component can have cascading effects across multiple public services. Failures in identity management may deny citizens access to essential services, inaccurate data exchanges may lead to exclusion, payment control deficiencies may compromise revenue integrity, and cyber incidents may disrupt service delivery across government. Consequently, technical vulnerabilities become public governance risks. For Supreme Audit Institutions (SAIs), the audit objective extends beyond assessing whether digital systems are operational to determining whether they operate lawfully, securely, inclusively, transparently, and accountably in delivering public value.

## 2. DPI and inclusive governance

Within the context of Digital Public Infrastructure (DPI), inclusive governance means that citizens can access, understand, use, and challenge public digital services, while obtaining timely redress where service failures occur. Digital inclusion extends beyond online availability; services must

remain accessible to individuals with limited connectivity, low digital literacy, disabilities, or inadequate devices, as well as to those relying on assisted service channels.

Kenya's digital transformation demonstrates the potential of Digital Public Infrastructure to advance inclusive governance. Platforms such as eCitizen, IFMIS, and the Social Health Authority have strengthened digital service delivery, public financial management, and access to health services through integrated digital channels (National Treasury, n.d.; Ministry of Health, 2025; Social Health Authority, n.d.-a).

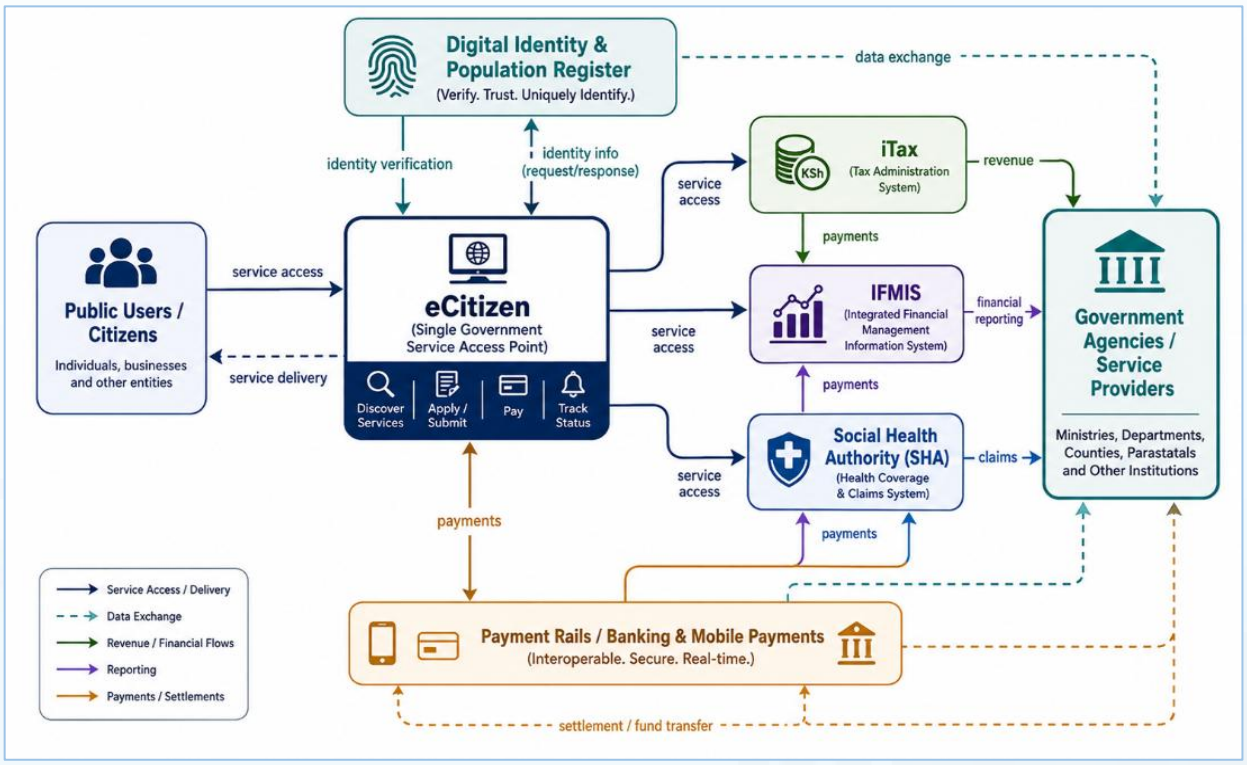



***Figure 1. Kenya's digital public infrastructure and key service links. Source: Author's illustration based on cited public sources.***

These developments demonstrate that DPI enhances efficiency by reducing transaction costs, improving record visibility, and strengthening service delivery. However, they also create concentration risk, whereby the failure of a shared identity, payment, or data exchange platform can disrupt multiple public services simultaneously. Effective interoperability enables integrated digital government, but it also requires robust governance, standardization, and accountability to prevent fragmented systems and ensure that digital investments deliver public value (ICT Authority, n.d.). Consequently, DPI influences who accesses government services, how public resources are distributed, how data is shared, and how citizens seek redress when digital services fail.

# 3. The main audit risks in a DPI environment

## 3.1 Inclusion and digital exclusion

The first audit risk is digital exclusion. While Digital Public Infrastructure (DPI) can expand access to public services, it may also disadvantage users who rely most on government services, including people living in low-connectivity areas, older persons, persons with disabilities, and individuals with limited digital literacy. For these groups, complex interfaces, lengthy digital forms, unstable network sessions, inaccessible system design, unclear user instructions, and weak complaint or appeal mechanisms can become significant barriers to service delivery.

The availability of multiple access channels does not, by itself, mitigate this risk. For example, the Social Health Authority (SHA) provides web-based, USSD, and assisted registration channels; however, auditors should assess whether these channels provide equitable access, operate consistently, and produce comparable outcomes for all users (Social Health Authority, n.d.-a). From an audit perspective, inclusion should be treated as a measurable control objective rather than a policy assertion. Accordingly, SAIs should evaluate whether public services can be effectively accessed using low-cost devices, unreliable internet connectivity, assistive technologies, and assisted service channels where digital self-service is not feasible.

## 3.2 Identity, eligibility, and wrongful denial

The second audit risk relates to weaknesses in identity and eligibility controls. Shared identity platforms reduce duplication and improve service targeting; however, deficiencies in identity matching, record updates, or verification processes may result in wrongful denial of public services. In Kenya, these risks have been subject to judicial scrutiny. The Court of Appeal held that the collection of DNA and GPS coordinates under the National Integrated Identity Management System (NIIMS) was intrusive and lacked sufficient legal justification unless supported by an appropriate regulatory framework (Mucheru & 2 others v. Katiba Institute & 2 others, 2022). Similarly, the implementation of the Huduma Card was suspended pending the completion of a Data Protection Impact Assessment in accordance with Section 31 of the Data Protection Act (Republic v. Joe Mucheru & 2 others; Katiba Institute & another (Ex parte), 2021).

These decisions demonstrate that digital identity systems are governance and constitutional mechanisms rather than merely technical databases. Accordingly, SAIs should assess controls over duplicate records, disputed identities, biometric matching errors, deceased records, and inaccurate or incomplete citizen information. Failure to detect and promptly resolve such errors may transform digital controls into barriers to citizens' rights and equitable access to public services.

## 3.3 Data governance and privacy

The third audit risk concerns ineffective data governance. DPI integrates data across identity, payment, registry, and service delivery platforms, enhancing operational efficiency while increasing the potential impact of control failures. Kenya's Data Protection Act requires data controllers to notify the Data Commissioner within seventy-two hours of a qualifying personal data breach and to investigate and determine complaints within ninety days (Data Protection Act, 2019). These statutory requirements elevate privacy from a legal obligation to a critical operational control.

Consequently, DPI audits should assess the lawful basis for processing, purpose limitation, access controls, data retention, third-party processing arrangements, breach notification procedures, complaint management, and protection of data subject rights. This is particularly important where sensitive personal information is processed. For example, the Social Health Authority (SHA) terms and conditions provide for verification of user information against government databases, use of multiple data sources for income assessment, reliance on third-party service providers, and possible service interruptions during maintenance (Social Health Authority, n.d.-b). Effective data governance should therefore be evidenced through documented controls, audit logs, contractual arrangements, and incident response procedures rather than policy statements alone.

## 3.4 Interoperability and data quality

The fourth audit risk relates to inaccurate data being propagated across interconnected systems. While interoperability is a fundamental objective of DPI, integration delivers value only where underlying data is accurate, timely, complete, and properly governed. Kenya's Government ICT Standards identify interoperability as a key enabler of integrated service delivery and information sharing across public institutions (ICT Authority, n.d.), making it both a strategic objective and an audit concern.

SAIs should therefore assess not only whether systems exchange data successfully but also whether the exchange is governed by effective controls. Audit procedures should examine data ownership, approval of corrections, documented interface specifications, validation controls, exception reporting, audit trails, and mechanisms that enable citizens to correct inaccurate records without repeated processing across multiple institutions. Where a government register is designated as the single source of truth, auditors should obtain sufficient evidence that it remains accurate, current, and authoritative.

## 3.5 Payment, Revenue, and Public Money Integrity

The fifth audit risk concerns the integrity of public financial transactions. Where DPI supports the collection of taxes, fees, contributions, claims, or other public payments, maintaining complete and accurate financial accountability becomes essential. Audit evidence should demonstrate that transactions are fully reconciled from user payment through financial institution settlement, accounting records, and reporting by the responsible public entity.

SAI Kenya, has reported variances between eCitizen revenue statements, the eCitizen platform, settlement reports, and government ledger balances (Office of the Auditor-General, 2024, 2025). These observations indicate that digital payment platforms do not eliminate financial risk; instead, they increase the complexity of assurance because transactions pass through multiple interconnected systems, financial institutions, and accounting processes.

Accordingly, SAIs should evaluate end-to-end reconciliations, segregation of duties, fee and tariff configuration, privileged access and override controls, refund processing, suspense accounts, settlement timeliness, and exception management. Where digital platforms interface with banks or payment service providers, audit procedures should follow the complete transaction lifecycle rather than focusing solely on the government application.

## 3.6 Cybersecurity, Business Continuity, and Vendor Dependence

The sixth audit risk relates to cybersecurity, operational resilience, and third-party dependence. Shared digital platforms are attractive targets because they process identity information, financial transactions, and sensitive government data at scale. The Communications Authority of Kenya reported that the National KE-CIRT/CC detected approximately 4.6 billion cyber threat events during the second quarter of the 2025/2026 financial year, attributing the increase to inadequate patch management, phishing attacks, and the growing use of AI-enabled threats (Communications Authority of Kenya, 2026). Consequently, cybersecurity should be considered both an information security and a public service continuity risk.

Cybersecurity is closely linked to vendor governance. The Social Health Authority's platform terms indicate reliance on government personnel and third-party service providers while acknowledging that maintenance activities and system outages may affect service availability (Social Health Authority, n.d.-b). Similar dependencies exist across many public digital platforms, where hosting, integration, maintenance, and security services are outsourced. These arrangements introduce risks relating to source code ownership, encryption key management, system logging, service-level performance, incident reporting, and exit strategies. SAIs should therefore assess digital resilience as an integrated governance, operational, and technical control objective rather than solely an ICT security function.

## 4. A Risk-Based Assurance Agenda for Supreme Audit Institutions

A risk-based audit approach should underpin the assurance framework for Digital Public Infrastructure (DPI). Given the extensive range of shared digital platforms, SAIs cannot audit every system simultaneously. Audit priorities should therefore be determined through risk assessment, focusing on platforms whose failure could result in significant public harm, financial loss, service disruption, compromise of sensitive data, or erosion of public trust. In the Kenyan context, these are likely to include shared identity, payment, taxation, health, and digital service delivery platforms.

A comprehensive assurance framework may be structured around six fundamental audit questions.

- **First, is the governance framework adequate?** Auditors should assess whether the legal mandate, institutional responsibilities, platform ownership, data stewardship, decision-making authority, and accountability arrangements are clearly defined. Weak governance structures create uncertainty, weaken oversight, and reduce auditability.
- **Second, is the platform inclusive and accessible in practice?** Audit evidence should extend beyond policy commitments to include walkthroughs, end-user journeys, accessibility assessments, assisted service channels, and analysis of complaints and appeals. Inclusive service delivery should be demonstrated through verifiable evidence rather than administrative assertions.
- **Third, are identity and eligibility controls effective?** Auditors should evaluate registration, identity verification, deduplication processes, exception handling, appeals, and correction mechanisms. Weak identity controls may result in wrongful denial of services, thereby undermining equitable access and public confidence.
- **Fourth, is data governed lawfully and securely?** Audit procedures should assess data collection, processing, sharing, retention, breach management, third-party processing, and protection of data subject rights. Compliance with statutory obligations under the Data Protection Act should form a core element of the assurance process.
- **Fifth, are financial transactions complete, accurate, and traceable?** For platforms processing government revenue, taxes, claims, or public contributions, auditors should obtain assurance that transactions can be traced from initiation through payment processing, settlement, accounting records, and financial reporting. This requires an integrated application of financial and information systems auditing.
- **Sixth, is the platform resilient and delivering public value?** Compliance alone does not demonstrate effectiveness. Auditors should evaluate system availability, operational resilience, business continuity, cost-effectiveness, user satisfaction, and achievement of intended outcomes. Consistent with ISSAI 100, ISSAI 300, and ISSAI 400, assurance over

Digital Public Infrastructure requires the integrated application of financial, compliance, performance, and information systems auditing. Such a multidisciplinary approach enables SAIs to determine whether DPI platforms operate lawfully, efficiently, securely, inclusively, and in a manner that delivers sustainable public value.




***Figure 2. Risk-based assurance agenda for auditing DPI. Source: Author's synthesis based on the audit risks and INTOSAI principles discussed in this article.***

## 5. Implications for Audit Design

The design of a Digital Public Infrastructure (DPI) audit should be centred on the public service journey rather than the underlying technology. Auditors should select a high-impact transaction such as tax filing, licence application, public fee payment, social benefit registration, or health claim and map the complete process from user access and identity verification through payment processing, back-office operations, record updates, notifications, and complaint resolution. This approach ensures that the audit assesses service delivery outcomes alongside the effectiveness of underlying controls.

Audit procedures should then trace both data and financial transactions by examining relevant legislation, contracts, system architecture, interface specifications, audit logs, exception reports, reconciliations, access records, incident reports, and complaint registers. Evidence should be

obtained through interviews with ICT personnel, system owners, frontline service providers, assisted-service agents, and end users. In a DPI environment, user experience provides an important source of audit evidence, as documented controls may not fully reflect operational effectiveness.

Audit recommendations should be practical, measurable, and risk-based. They should clearly identify the responsible institution, the required corrective action, expected performance outcomes, implementation timelines, and follow-up arrangements. Examples include establishing comprehensive service inventories, assigning ownership of system interfaces, conducting periodic disaster recovery testing, monitoring service availability, and reporting performance indicators such as complaint resolution and data correction timelines.

## 6. Conclusion

Digital Public Infrastructure has transformed public administration by improving accessibility, transparency, transaction traceability, and the efficiency of service delivery. However, while these benefits enhance public sector performance, they also introduce new governance, financial, operational, and cybersecurity risks. Weak identity controls may result in exclusion from public services, ineffective data governance may compromise privacy, inadequate financial controls may undermine revenue integrity, and limited cyber resilience may disrupt critical government services.

These risks require Supreme Audit Institutions (SAIs) to adopt a multidisciplinary, risk-based assurance approach. DPI should be audited as critical public infrastructure that underpins governance rather than as a standalone technology initiative. Such an approach enables SAIs to assess legality, accountability, inclusion, data integrity, financial integrity, operational resilience, and the achievement of intended public outcomes.

Ultimately, the effectiveness of Digital Public Infrastructure should not be measured solely by the number of services delivered or the speed of transaction processing. Rather, its success should be evaluated by whether it operates lawfully, securely, reliably, inclusively, and transparently while delivering sustainable public value. By applying the principles of the ISSAI Framework through integrated financial, compliance, performance, and information systems auditing, SAIs can strengthen accountability, reinforce public trust, and promote inclusive digital governance.

## References


Communications Authority of Kenya. (2026). *Second quarter sector statistics report for the financial year 2025/2026*. https://www.ca.go.ke/sites/default/files/2026-04/Sector%20Statistics%20Report%20Q2%202025-2026.pdf

Data Protection Act, No. 24 of 2019 (Kenya). https://new.kenyalaw.org/akn/ke/act/2019/24/eng@2022-12-31

eCitizen. (n.d.). *Government of Kenya services simplified*. https://accounts.ecitizen.go.ke/

Executive Office of the President. (2023). *Executive Order No. 2 of 2023*. https://www.president.go.ke/wp-content/uploads/Executive-Order-No.-2-of-2023-.pdf

ICT Authority. (2022). *Kenya National Digital Master Plan 2022–2032*. https://cms.icta.go.ke/sites/default/files/2022-04/Kenya%20Digital%20Masterplan%202022-2032%20Online%20Version.pdf

ICT Authority. (n.d.). *Government ICT standards*. https://www.icta.go.ke/ict-standards

International Organization of Supreme Audit Institutions. (2019a). *ISSAI 100: Fundamental principles of public-sector auditing*. https://www.issai.org/wp-content/uploads/2019/08/ISSAI-100-Fundamental-Principles-of-Public-Sector-Auditing-1.pdf

International Organization of Supreme Audit Institutions. (2019b). *ISSAI 300: Performance audit principles*. https://www.issai.org/wp-content/uploads/2019/08/ISSAI-300-Performance-Audit-Principles.pdf

International Organization of Supreme Audit Institutions. (2019c). *ISSAI 400: Compliance audit principles*. https://www.issai.org/wp-content/uploads/2019/08/ISSAI-400.pdf

Ministry of Health. (2025, February 26). *Taifa Care media update*. https://www.health.go.ke/sites/default/files/2025-02/Press%20Release_State_of_Health_260225.pdf

*Mucheru & 2 Others v. Katiba Institute & 2 Others* (Civil Application E373 of 2021) [2022] KECA 386 (KLR) (4 March 2022). https://kenyalaw.org/akn/ke/judgment/keca/2022/386/eng@2022-03-04

National Treasury. (n.d.). *Integrated Financial Management Information System (IFMIS).* https://www.treasury.go.ke/ifmis

Office of the Auditor-General. (2024). *Auditor-General's summary report on national government, 2022/2023*. https://www.oagkenya.go.ke/wp-content/uploads/2024/06/AUDITOR-GENERALS-SUMMARY-REPORT-ON-NATIONAL-GOVERNMENT-2022-2023-with-cover.pdf

Office of the Auditor-General. (2025). *Auditor-General's summary report on national government, 2023/2024*. https://www.oagkenya.go.ke/wp-content/uploads/2025/04/Auditor-Generals-summary-Report-on-National-Government-2023-2024.pdf

*Republic v. Joe Mucheru & 2 Others; Katiba Institute & Another (Ex parte)* [2021] KEHC 122 (KLR) (14 October 2021). https://kenyalaw.org/akn/ke/judgment/kehc/2021/122

Social Health Authority. (n.d.-a). *Social Health Authority*. https://sha.go.ke/

Social Health Authority. (2024, June 1). *Social Health Authority platform terms and conditions*. https://sha.go.ke/media/SHA_Terms_and_Conditions.pdf

United Nations Development Programme. (2023). *The DPI approach: A playbook*. https://www.undp.org/publications/dpi-approach-playbook

World Bank. (2025). *Digital public infrastructure and development: A World Bank Group approach*. https://openknowledge.worldbank.org/entities/publication/cca2963e-27bf-4dbb-aa5a-24a0ffc92ed9

# Beyond IS Audit

*Auditing the Invisible Architecture of Digital Public Infrastructure*


## Ajay Yeshwanth

O/o the Comptroller & Auditor General of India




A citizen in a small town today may never see the machinery of government at all: no queue, no counter, no file moving between desks. She establishes her identity through a number linked to her biometric identity. She receives a subsidy through a bank account linked to that number. She books a hospital appointment, files a tax return, or accesses a land record through a platform she has never had to understand. This is Digital Public Infrastructure (DPI) at work: the identity, payment, data-exchange, trust, and discovery layers that increasingly sit underneath the whole of government service delivery, not as an occasional IT project bolted onto a department, but as the default architecture through which the state now reaches its citizens.

Government systems, in other words, have stopped being linear. A welfare scheme is no longer one department's database; it is an identity platform, a payments rail, a beneficiary registry, and two or three private-sector intermediaries, all exchanging data in real time. Auditing this requires auditors to keep pace with an architecture that did not exist, in this form, a decade ago, and the stakes of getting that oversight right have only grown. Under India's Digital Personal Data Protection Act, 2023, and comparable regimes taking shape across the world, DPI systems now hold enormous volumes of citizens' personal and confidential data. Auditing how that data is governed is no longer a technical footnote to a performance audit; it is close to the centre of what public accountability means in a digital state. It was to address this challenge that SAI India, as part of an ASOSAI pledge, led the initiative to develop the DPI Audit Guidelines, now available on the iCISA website. What follows is an inside account of that process, the deliberations the SAI India team worked through, and the choices we weighed, in arriving at the framework that resulted.

## From IS Audit to a New Discipline

Supreme Audit Institutions have audited information systems for decades, and SAI India's own IS audit practice, reflected in guidance such as IS Audit Manual, is mature and well understood. DPI audit grows out of that tradition, but it is not simply IS audit under a new name. An information system, however large, is usually one system: a defined boundary, one custodian, one set of controls to test. A DPI is rarely that. It is several systems, an identity registry, a payments switch, a consent layer, a departmental application, built and run by different entities, talking to each other continuously through APIs and shared standards. The audit's unit of analysis shifts from a system to an ecosystem. That shift created the need for the DPI Audit Guidelines as a distinct body of guidance rather than an addendum to existing IS audit instructions.

## Where This Began

The mandate for this work came through ASOSAI, the Asian Organisation of Supreme Audit Institutions, against the backdrop of INTOSAI's wider push to build audit capability for digital government. SAI India was a natural pen-holder for two reasons that rarely coincide in one institution. As an implementer, India has run DPI at a scale few countries can match: Aadhaar, UPI, DigiLocker, and the Account Aggregator framework are not distant case studies but systems operating in our own backyard. As a Supreme Audit Institution, India chairs INTOSAI's Working Group on IT Audit and hosts iCISA, its designated Global Training Facility for IT audit, giving us both the platform and the standing to convene this work on behalf of the wider SAI community, rather than write it for India alone.

## The Fulcrum: People, Process, Tools & Technology, Data Governance

Everything in the Guidelines turns on a single analytical lens: (People, Process, Tools & Technology, and Data Governance) PPT&D. It is not a new idea in audit; what is deliberate is the fourth pillar. Data Governance is not folded into 'Technology' as a subordinate concern, the way it often is in conventional IS audit frameworks. It stands as a full and equal pillar, tracked across its own lifecycle (creation, use, sharing, retention, disposal) because in a DPI, what happens to a citizen's data after collection is very often where the real risk sits. The same lens applied consistently across governance, stakeholder engagement, and citizen-facing risk is also what lets the framework surface duplication, fragmentation, overlap, and gaps across institutions: weaknesses that stay invisible when auditors examine one agency or one system at a time.

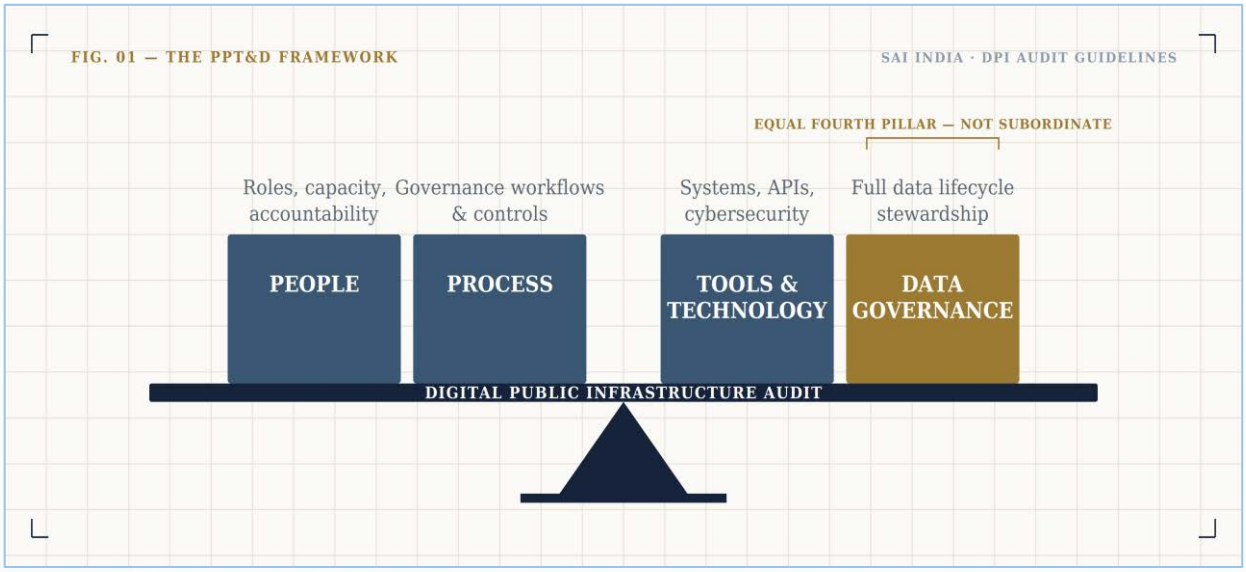



*Figure 1: The PPT&D framework, the fulcrum of DPI audit.*

## Standing on Global Consensus

PPT&D supplies the lens; it does not stand alone. The Guidelines are built as four interconnected layers. ISSAI 100, 3000, 4000, and GUID 5100 supply the mandatory professional foundation: how a DPI audit is planned, evidenced, and reported does not depart from how any SAI audit is planned, evidenced, and reported. The UN Universal DPI Safeguards Framework (2024), currently the closest thing the international community has to an agreed baseline for DPI governance, deliberately light enough to avoid over-regulating a still-evolving technology, supplies the content: its eighteen principles and thirteen risk categories, clustered under inclusion, safety, and structural integrity, shape what the Guidelines actually ask auditors to look for. ISO and OECD standards (27001, 27701, 22301, 15489, 8000, 9241, and WCAG 2.1 among them) supply the specific control benchmarks within each PPT&D dimension. None of this is a citation list appended for authority: every one of these instruments is traceable to a specific section, sub-objective, or Audit Design Matrix entry, so an auditor can start from any of the four layers and find their way to the others.




*Figure 2: The four-layer architecture set out in Section 1.6 of the Guidelines.*

## The Hard Choices

The most difficult decisions in drafting were not about what to include, but the appropriate level of abstraction. A guideline specific enough to be usable on Monday morning by an auditor beginning their first DPI engagement risks being unusable by a SAI where DPI is still nascent, or a federated state with governance distributed across regulators rather than concentrated in one authority. We resolved this by calibrating rather than choosing: the audit objectives explicitly presuppose a mature DPI ecosystem, but the Guidelines set out how auditors should scale the same objectives down for early-stage or institutionally fragmented environments, prioritising foundational governance safeguards over full operational benchmarks where the underlying institutions are still forming. The audit guideline stays genuinely one document, not two, but it is built to bend.

## Tested by the ASOSAI Community

None of this was written in isolation. Before publication, the draft went to ASOSAI member SAIs for formal comment across two rounds of consultation, and that dialogue shaped the Guidelines as much as the initial drafting did. Roughly two-thirds of what came back as feedback led directly to a change, or pointed to something the team then made clearer. The rest opened up genuinely valuable conversations around certain design choices - why the framework stays technology-neutral rather than naming a specific control methodology, why risk is judged qualitatively rather than through a numeric score, why audit independence is kept distinct from investment appraisal - and each of those conversations left the reasoning behind the Guidelines sharper and

easier for any reviewing SAI to apply. It is that continuing exchange with the ASOSAI community, as much as the original drafting, that gives the Guidelines their credibility.

## A Ready Reference: Five Layers, Eight Sectors

Because DPI is still an unfamiliar audit domain for most auditors, these Guidelines do not assume prior fluency. Before an auditor reaches methodology, the document builds up the basic architecture of DPI itself: what these systems are, how they differ from a conventional application, and why. From there, the Guidelines organise around five core components common to most DPI stacks (identity, trust and authentication, payments, data exchange, and discovery and fulfilment) and extend the same logic across eight sectors where DPI is now doing real work: health, education, agriculture, land records, taxation, urban governance, e-commerce, and procurement. Annexures E and F turn each of these into a ready reference: specific, illustrative audit questions an auditor can open on day one, rather than derive from first principles.

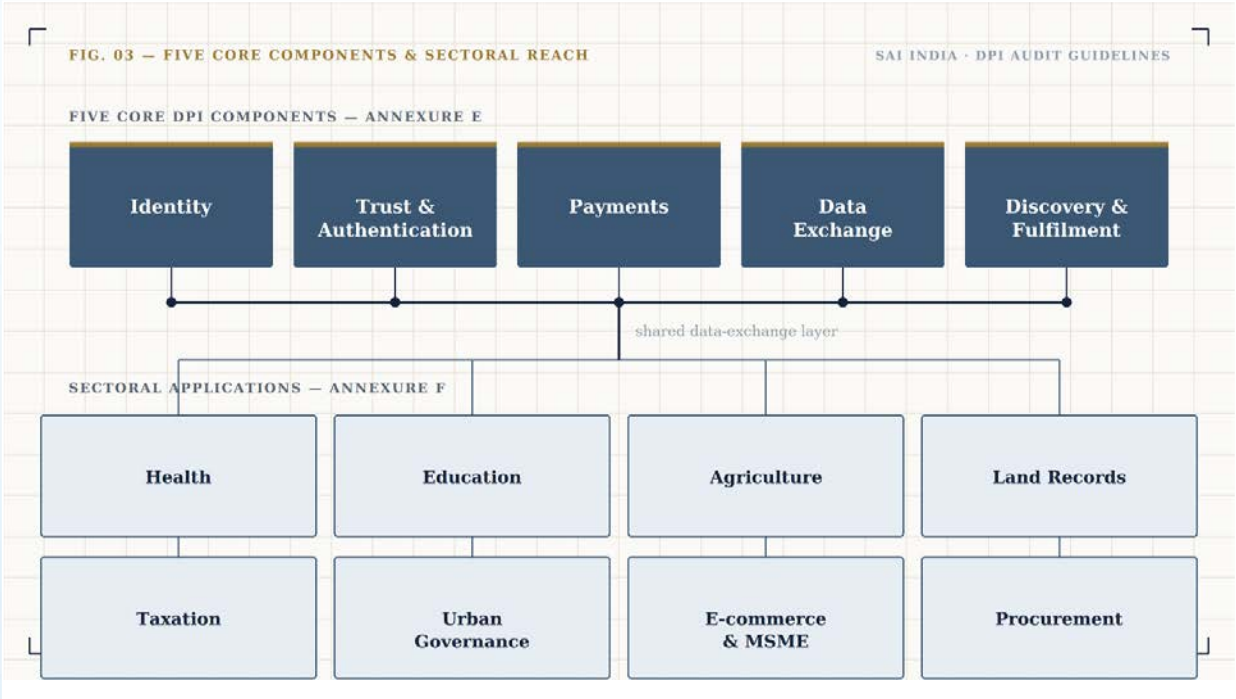



*Figure 3: The five core DPI components (Annexure E) and their extension across sectors (Annexure F).*

## Three Objectives, One Integrated Audit

The audit objectives themselves are organised into three domains (Governance of DPI, Engagement with Stakeholders, and Inclusion, Access & Privacy for Citizens), each mapped back to PPT&D and to a phase of the data lifecycle. The third deserves particular attention: rather than treating privacy as a specialist compliance concern bolted onto a performance audit, the Guidelines fold it into the same objective as inclusion and access, on the reasoning that a DPI

that is not privacy-respecting cannot, by definition, be delivering equitable access: a system citizen cannot trust is one they will quietly avoid using.

The Guidelines then draw all three together into a single worked audit approach, and are explicit that this should not be conducted as three separate exercises. A DPI audit is recommended as a single integrated engagement (performance, compliance, and information-systems audit combined) because a finding on governance, a finding on a stakeholder contract, and a finding on data retention are very often symptoms of the same underlying weakness.




*Figure 4: The three audit objectives converge into a single integrated audit engagement.*

## From Paper to Practice: The UPI Pilot

The clearest test of any framework is whether it survives contact with a real system. SAI India is already running a pilot DPI audit of the Unified Payments Interface, applying PPT&D to one of the country's most heavily used payment rails. It is early, but it is already doing what a pilot should: telling us where the framework's language needs sharpening before the next SAI picks it up.

## Building the Global Workforce: iCISA and CADS

A guideline is only as useful as the auditors applying it, and that has deliberately not been left to chance. Much of what DPI audit asks for is an extension of skills IS auditors already have (testing controls, tracing evidence, assessing risk) applied to an ecosystem rather than a single system. What is genuinely new sits largely within Objective 3: assessing privacy by design, data minimisation, and citizen-facing accessibility as audit criteria in their own right, not as a specialist add-on.

iCISA, INTOSAI's designated Global Training Facility for IT audit, is the natural home for building that capability for SAIs everywhere, and SAI India is going a step further at home. CADS (Certification on Audit of Digital Systems, under development with IIT Madras) includes a domain combining DPI audit with data privacy and protection audit as a single competency track, tiered from foundation to expert. We are not aware of a comparable global certification that treats DPI audit and privacy audit as one discipline rather than two adjacent ones; if that holds, it may prove as significant a contribution as the Guidelines themselves.

## What Comes Next

The Guidelines describe themselves, deliberately, as a living document. AI is already layering itself onto DPI, through automated eligibility decisions and algorithmic fraud detection, faster than any single framework can be revised to match. Cross-border interoperability between national DPI stacks is only beginning. And the peer review process that shaped this first edition does not end with publication; it is, if anything, the template for how the next one should be written. The invisible architecture our citizens now depend on will keep changing. The job, for all of us, is to make sure the audit keeps pace with it.

### References

SAI India, Digital Public Infrastructure (DPI) Audit Guidelines, April 2026. • UN Universal DPI Safeguards Framework (2024). • INTOSAI: ISSAI 100, ISSAI 3000, ISSAI 4000, GUID 5100. • ISO/IEC 27001, ISO/IEC 27701, ISO 22301, ISO 15489, ISO 8000, ISO 9241; WCAG 2.1. • Digital Personal Data Protection Act, 2023 (India).

# Digital Public Infrastructure as an Enabler of Inclusive Governance: Opportunities, Risks, and the Role of Audit



**Pranay Chauhan**
Faculty at ICAI Digital Accounting and Assurance Board (DAAB), India

## Abstract

Digital Public Infrastructure (DPI) has become a defining feature of modern governance. By building shared digital platforms for identity, payments, and data exchange, governments can now deliver public services at a scale and speed that were previously impossible. For citizens who have historically been excluded from formal systems, DPI creates a genuine pathway to economic participation and access to state support. Yet this scale also introduces serious risks. A single vulnerability in a shared infrastructure layer can cascade across multiple services and affect millions of people simultaneously. This paper examines what DPI means for inclusive governance, the risks it brings, and why Supreme Audit Institutions (SAIs) have a critical role in providing independent assurance over these systems. It concludes that the promise of inclusive governance through DPI is achievable only when the infrastructure is governed with integrity and audit is one of the most important mechanisms for ensuring this objective.

## Keywords

Digital Public Infrastructure, IT Audit, Cybersecurity, Inclusive Governance, Data Protection.

## 1. Introduction

Governments across the world are investing in shared digital platforms, common foundations for identity, payments, and data exchange that multiple agencies and services can use simultaneously. This approach, widely known as Digital Public Infrastructure, has shifted rapidly

from policy concept to global governance reality. Countries across Africa, Southeast Asia, and Latin America have drawn on early DPI experiences to build their own foundational digital systems (World Bank, 2022; UNDP, 2023).

A single trusted identity layer can serve every ministry, eliminating the need for each agency to build its own. A unified payment infrastructure can process all welfare transfers through one channel. Citizens avoid navigating multiple portals and carrying stacks of physical documents. Services become faster, more cost-effective, more consistent, and more accessible to people.




**Figure 1.1: Core Components of Digital Public Infrastructure**

However, shared infrastructure carries shared risk. A failure or breach at the DPI layer does not remain contained, it cascades across every service that depends on it. Supreme Audit Institutions have a direct responsibility to ensure that DPI systems are well governed, properly secured, and genuinely serving the populations they are designed for. This paper explains what that responsibility entails in practice.

## 2. DPI and Inclusive Governance

Inclusive governance is fundamentally about the state's ability to reach all citizens, including those who are underprivileged, remote, undocumented, or outside the formal economy. For decades, this was primarily a physical challenge: how do you deliver a government service to someone in a remote area without a bank account or formal identity document.

DPI addresses this challenge through digital means. A biometric identity system can register someone who has never held official documentation. A mobile payment platform can transfer welfare funds directly to recipients without requiring a nearby bank branch. A digital document wallet eliminates the need for repeated visits to government offices. When designed with inclusion as a core objective, DPI does not simply digitize existing services; it extends access to people who were previously excluded (World Bank, 2022; IMF, 2023).

However, DPI does not automatically deliver inclusion. Poor digital literacy, unreliable internet access, language barriers in digital interfaces, and biometric matching failures can exclude the very populations the system is designed to serve (OECD, 2022; UNDP, 2023).

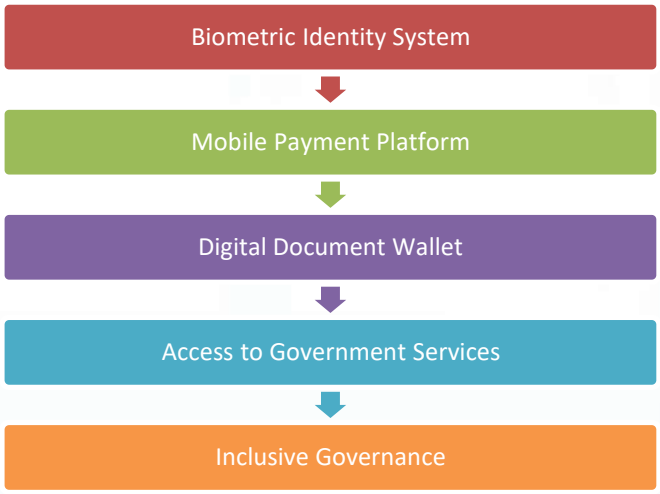



**Figure 2.1: DPI Pathway to Inclusive Governance**

## 3. The Risk Landscape of DPI

The risks associated with DPI fundamentally differ from those of standard government IT systems. A conventional departmental system serves a single function for one agency; if it fails, the impact is bounded and localized. DPI is deliberately built to be shared and interoperable across many services and agencies simultaneously. This shared nature is precisely what makes it powerful. It also makes its risk profile distinctly more serious and complex (ISACA, 2019).




**Figure 3.1: Major Risks Associated with DPI**

## 3.1 Systemic Risk

Because DPI serves as a shared foundation for many services simultaneously, a failure at the infrastructure level cascades across all dependent services. A disruption to a national identity authentication service could simultaneously block citizens from accessing banking, healthcare, welfare payments, and government portals. This type of systemic, cascading risk is not adequately addressed by conventional IT risk frameworks, which typically assess systems individually rather than assessing interconnected dependencies (ISACA, 2019).

## 3.2 Cybersecurity Threats

DPI systems operating at a national scale are high-value targets for sophisticated threat actors. State-sponsored actors and organized criminal groups actively seek to penetrate infrastructure that handles identity verification and financial transactions for entire populations. The threat landscape includes attacks on authentication mechanisms, interception of transaction data, manipulation of beneficiary records, and large-scale fraud through stolen credentials. Distributed denial-of-service attacks on payment infrastructure can disrupt economic activity far beyond the reach of any single organization (WEF, 2023).

## 3.3 Data Privacy and Consent

DPI systems process enormous volumes of sensitive personal data, including biometric records, financial transaction histories, health information, and legal documents. Unauthorized access, sharing without informed consent, and retention beyond necessary periods represent serious risks. Where data protection legislation is in force, compliance with statutory requirements is a direct and material audit concern (Zwitter & Gstrein, 2020; European Commission, 2022).

## 3.4 Third-Party Integration Risk

DPI is intentionally built to be open, so private sector participants can connect through application programming interfaces (APIs). This approach drives innovation and extends service reach, but it also means that the security of the entire ecosystem depends on every organization that connects to it. A vulnerability introduced by a single third party integrator can become an entry point into the broader DPI infrastructure, potentially compromising the entire system.

## 3.5 Exclusion Through Technical Failure

For citizens who depend on DPI enabled services for basic needs, system failures are not merely technical inconveniences; they represent hardships. A citizen who cannot authenticate their identity may be unable to access food rations or collect welfare benefits. A family whose welfare transfer fails during a system outage faces genuine difficulty. The risk of exclusion through

technical failure deserves the same audit attention as fraud or security breaches, as it directly undermines the inclusive governance objective.

## 4. The Audit Mandate and Key Focus Areas

Supreme Audit Institutions exist to provide independent assurance that government systems work as intended, that public funds are used properly, and that citizens' rights and interests are protected. All three mandates apply directly to DPI. DPI involves substantial public investments in both the infrastructure itself and the government services that depend on it. It involves significant delegated authority. when a government deploys a digital identity system, it entrusts the power to authenticate citizens to a technology platform. These systems hold the most personal aspects of citizens' lives: their identities, financial histories, and health records. Audit institutions carry clear responsibility across all three dimensions (INTOSAI Development Initiative, 2022).

The six areas in Table 1 represent the most important focus points for a comprehensive DPI audit.

| Audit Focus Area | Key Questions for Auditors |
|---|---|
| Governance and Accountability | Is there clear ownership and responsibility for DPI? Are decision-making processes documented and transparent? Are there effective mechanisms for receiving and addressing citizen complaints? |
| Technical Security and Controls | Are authentication systems robust and tested? Are access logs generated and reviewed? Is data encrypted in transit and at rest? Are third-party integrations properly validated? |
| Data Protection Compliance | Is personal data collected only as necessary? Is data retention limited to specified periods? Are data-sharing agreements in place and reviewed? Is consent properly obtained and documented? |
| Business Continuity and Resilience | Are continuity plans tested and up-to-date? Can the system recover from failures within acceptable timeframes? Are backup systems maintained? Is disaster recovery capability verified? |
| Inclusion and Service Delivery | Are services reaching intended beneficiaries? Are exclusion rates tracked and investigated? Are there accessible grievance mechanisms? Is digital literacy support provided where needed? |
| Compliance and Legal Framework | Are system operations compliant with data protection laws? Are regulatory reporting requirements met? Are audit trails maintained to support compliance verification? |

## 5. Communicating Findings and Building Audit Capacity

DPI audit findings are often technically complex and institutionally sensitive. Communicating them effectively means connecting technical observations to governance consequences. A finding about untested continuity arrangements carries greater weight when it estimates how many citizens would lose access to essential services during an outage.

DPI findings often involve multiple responsible parties: the core DPI operator and connected third-party integrators. Clear attribution of responsibility and identification of required corrective action from each party are essential if findings are to drive real change. Public audit reports in this domain can also help citizens understand their digital rights and hold infrastructure operators accountable, but the language must be accessible to ordinary readers, not only technical specialists (IDI-WGITA, 2022).

Auditing DPI effectively requires capabilities that many audit institutions are still developing. The domain sits at the intersection of public administration, cybersecurity, data protection law, and citizen service delivery. Audit institutions need to invest in technical skills, including network security, cloud architecture, API design, and data analytics. Collaboration with national cybersecurity bodies and data protection authorities can fill expertise gaps that are difficult to address in-house.

## 6. Conclusion

DPI holds genuine promise as a tool for inclusive governance. It can reach citizens who have historically been excluded, lower the cost and complexity of public service delivery, and create more transparent systems for distributing public benefits. However, realizing this promise requires more than well-designed technology. It requires a trustworthy governance infrastructure that is secure, resilient, transparent, and accountable to the people it serves.

### References


- Datta, P. (2023). Digital public infrastructure and inclusive development: Evidence from low and middle-income countries. Journal of Development Policy and Practice, 8(1), 45–67.
- European Commission. (2022). Digital public services and infrastructure: A framework for assessment. Publications Office of the European Union.
- INTOSAI Development Initiative and Working Group on IT Audit (IDI-WGITA). (2022). Handbook on IT audit for Supreme Audit Institutions. INTOSAI.
- ISACA. (2019). COBIT 2019 framework: Introduction and methodology. ISACA.
- International Monetary Fund (IMF). (2023). Digital infrastructure and financial inclusion in emerging economies. IMF Working Paper WP/23/112.

- OECD. (2022). Digital government index: 2021 results. OECD Public Governance Policy Papers, No. 24. OECD Publishing.
- United Nations Development Programme (UNDP). (2023). Digital public infrastructure for sustainable development. UNDP Global Policy Network.
- World Bank. (2022). Digital public infrastructure: The emerging market experience. World Bank Group.
- World Economic Forum (WEF). (2023). Advancing digital public infrastructure: A framework for governments. WEF White Paper.
- Zwitter, A., & Gstrein, O. J. (2020). Big data, privacy and COVID-19: Learning from humanitarian expertise in data protection. Journal of International Humanitarian Action, 5(1), 1–7.




Section V(B)

# FIELD EXPERIENCE

# Auditing Digital Public Infrastructure: Lessons from TCU (SAI Brazil) on Quality Assessment of Selected Federal Digital Services[4]



**André Luiz de Albuquerque Farias**
Federal Court of Accounts, Brazil

## Abstract

Digital Public Infrastructure (DPI) is a foundational enabler of inclusive, efficient, and accountable governance. In 2024, Brazil's Federal Court of Accounts (TCU) conducted a performance audit evaluating the quality of four high-demand federal digital services: (i) *Meu SUS Digital*[5] (Health); (ii) Disability Assistance Benefits[6] (Social Security); (iii) National High School Exam (ENEM)[7] (Education); and (iv) Online Police Report (DEVIR)[8] (Public Security). Using a methodology composed of technical adherence to digital standards and user-perceived quality TCU found significant governance gaps. Main findings included: (1) management support tools, including the *Gov.br*[9] satisfaction evaluation API[10] and the federal ombudsman platform (*Fala.br*), were not used by service managers to drive improvement; (2) performance monitoring dashboards lacked mandatory indicators; and (3) strategic targets remained unmet. This article contextualises these findings within international DPI frameworks, benchmarks them against

4 Case number TC 002.007/2024-0; audit report approved by Decision 744/2025.

5 A digital health solution offered by the Brazilian Unified Health System ("SUS") designed to facilitate access to health information, allowing users to track their medical history, vaccination data, test results, medications, transplant waiting list position, and other services.

6 Classified as a Continuous Benefit Payment (known as "BPC" in Brazil).

7 ENEM is the largest educational assessment in Brazil and the main gateway to higher education. Its scores are used for admission to public universities, obtain scholarships at private institutions and apply for student loans.

8 Known in Brazil as DEVIR, which means *virtual police station*.

9 *Gov.br* is the unified platform of the Brazilian Federal Government created to centralize and facilitate citizens' access to digital public services and government information.

10 Application Programming Interface (API) is a collection of definitions and protocols used to create and integrate application software.

INTOSAI and OECD good practices, and proposes key elements to be considered for SAI Audit Frameworks, and also future audit work focused on DPI Governance.

## Keywords

digital public infrastructure; e-government; digital public services; performance audit.

## Introduction

The concept of Digital Public Infrastructure (DPI) has gained significant traction in global development and governance agendas. Defined by the G20 Digital Economy Working Group (2023) as open, interoperable, and secure digital systems that serve as building blocks for public and private service delivery, DPI encompasses identity systems, data-exchange layers, payment platforms, and the ecosystem of citizen-facing digital services built upon them.

When well-governed, DPI can accelerate the Sustainable Development Goals (SDGs), particularly SDG 16 (Peace, Justice and Strong Institutions) and SDG 10 (Reduced Inequalities), by reducing barriers to accessing government services and ensuring that no citizen is left behind (UNDP, 2023).

Brazil has invested substantially in its national DPI over the past decade. *Gov.br*, for example, the unified digital identity and service portal, now hosts nearly 4,900 federal services for over 160 million registered users (SGD, 2024), complemented by a satisfaction evaluation service[11], the *Fala.br* ombudsman platform, and sector-specific applications including *Meu SUS Digital*, ENEM, BPC, and DEVIR. Together they constitute a multi-layered DPI reaching virtually every Brazilian citizen. Yet DPI is only as effective as the governance mechanisms that sustain, monitor, and continuously improve it.

In 2024, the Audit Unit specialised in Information Technology (AudTI) of TCU conducted a performance audit to evaluate the quality of four selected highly demanded federal digital services (TCU, 2024). The findings illuminate a common paradox shared by many emerging DPI ecosystems: substantial investment in infrastructure without proper investment in the feedback and accountability loops that make that infrastructure genuinely inclusive and responsive.

Given this scenario, the purpose of this article is, through a case study based on one of the most recent performance audit reports in key DPI services in Brazil, present the audit's design, key findings, and their implications for the broader SAI community. Moreover, we try to discuss the relevance of the Brazilian case within international DPI literature, benchmark the findings against INTOSAI and OECD good-practice standards, and contribute a short, replicable table of key audit elements to be used by SAIs worldwide when assessing DPI governance maturity.

[11] Including an API for third parties access register, consult and process complaints.

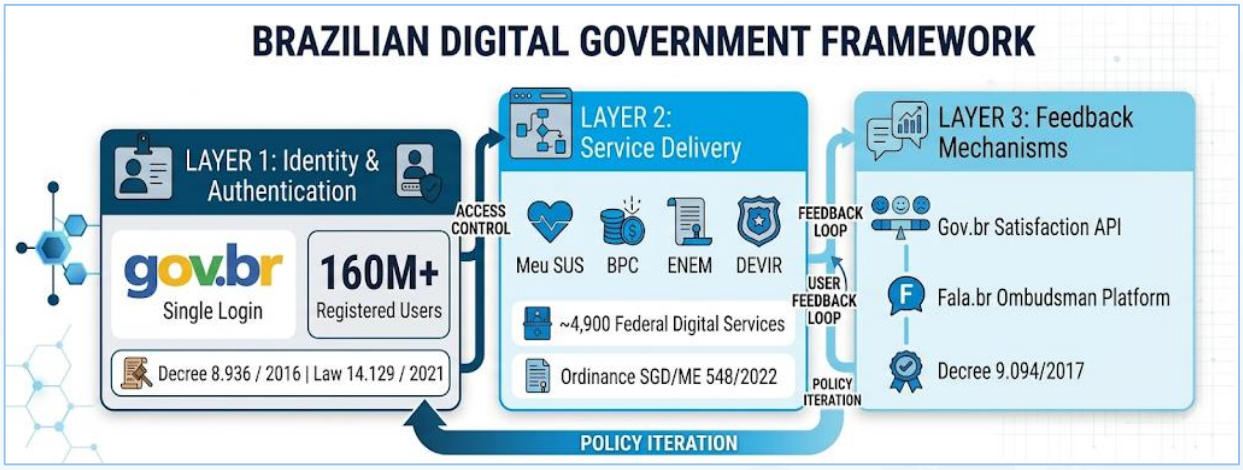
## Digital Public Infrastructure: Conceptual Framework

DPI encompasses the foundational digital systems upon which governments and private actors build services at population scale (Dempsey et al., 2022). The GovStack initiative (ITU and GIZ, 2022) extends the standard three-layer model (identity, payments, data exchange) to include service delivery platforms and feedback/grievance mechanisms.

In this case study, *Gov.br* serves as the identity layer (SSO), the satisfaction API and *Fala.br* constitute the feedback layer, and the four audited services (*Meu SUS Digital*, BPC, ENEM, and DEVIR) represent the citizen-facing delivery layer.

Following Banga and te Velde's (2021) stacked DPI concept, the value of each layer depends critically on the governance integrity of the layers as shown in Figure 1:

***Figure 1. Simplified Brazil's DPI architecture of selected services***




*Source: Author's elaboration, based on TCU's Audit Report and GovStack DPI Framework.*

Heeks (2018) warns that e-government failure risk rises sharply when a design-reality gap exists between digital systems and citizens' lived realities, which is precisely the vulnerability the TCU audit exposed in this case. Ndou (2004) found that technical deployment in developing countries routinely outpaces institutional capacity for feedback integration, while Bannister and Connolly (2012) argue that digital government legitimacy depends on demonstrated responsiveness to user experience.

Mergel et al. (2019) define digital transformation as a process demanding organisational change, not merely technology adoption. The OECD Digital Government Policy Framework (OECD, 2020) identifies six maturity dimensions — including citizen-driven design and data-driven government — all of which require functioning feedback loops. INTOSAI's ISSAIs 20 and 5300 provide the normative SAI framework for evaluating whether DPI delivers on its inclusive governance promise, requiring auditors to assess not only technical functionality but equity, transparency, and citizen responsiveness (INTOSAI, 2019; WGITA, 2022).

## The TCU Audit: Scope and Methodology

The SAI Brazil audit was conducted by the Specialized Information Technology Audit Unit of the TCU (AudTI) between February and July 2024, covering six main federal entities, including the Digital Government Secretariat (SGD), the Comptroller General of the Union (CGU), National Institute of Social Security (INSS), and the Ministries of Health, Justice, and Education. Four services were selected for this audit: *Meu SUS Digital* (health records), request for continuous disability payment (BPC), ENEM's request (university standard entrance exam), and online police crime reporting (DEVIR).

Service selection applied criteria of national coverage, *Gov.br* satisfaction API integration, non-immediacy of delivery, and existence of user advisory councils, ensuring a representative sample across social, security, and education domains. The audit adopted a dual-quality framework: (1) User-perceived quality: measured through focus groups and a structured *Lime Survey* questionnaire covering clarity, language, channels, usability, and overall satisfaction; and (2) Technical quality: assessed via manager questionnaires evaluating *Gov.br* API adherence, accessibility (eMAG), data protection (LGPD[12]), Design System adoption, and interoperability, normalised to a 1–5 scale.

The audit also extended its scope to evaluate the systemic quality infrastructure: the federal monitoring dashboard, the *Fala.br* ombudsman platform, and progress toward the Digital Government Strategy (DGS) targets[13]. This broader scope turned the audit from a simple service-level assessment into a DPI governance audit directly relevant to the WGITA theme of DPI as an enabler of inclusive governance.

## Key Audit Findings

### 1. Management Support Tools Are Ineffective for Improving Digital Services

The first and most structurally significant finding concerns the breakdown of the DPI feedback loop. Despite Brazil's legal framework explicitly mandating that the *Gov.br* satisfaction evaluation API be used by service managers to guide continuous improvement, none of the four audited service managers cited the API as an input in their improvement processes even when directly questioned.

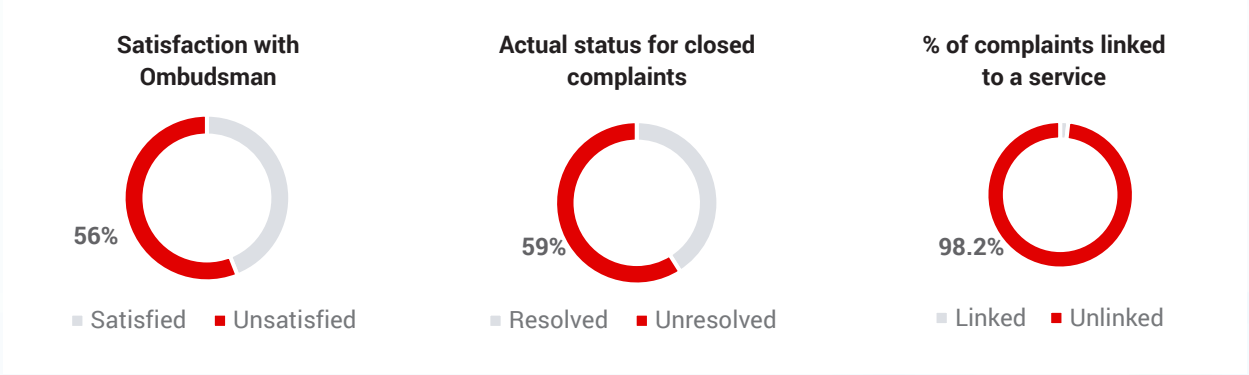
Three interconnected failure points emerged in this audit. At the data layer, the API lacked a free-text field and used generic questions rather than service-specific ones. At the ombudsman layer, less than 1.8% of *Fala.br* complaints could be linked to a specific service; citizens wishing to escalate faced full re-authentication and needed to re-enter information already known to

12 Brazil's General Data Protection Law.
13 Decree 10.332/2020.

the system. At the institutional layer, user advisory councils existed for only 5% of digital services and 83% of those had fewer than nine members.

The downstream effect is documented in the ombudsman data: 56% of citizens surveyed expressed dissatisfaction with the ombudsman service, and 59% of complaints were closed without resolution, a feedback loop failure that erodes public trust in digital government and is directly confirmed by the TCU findings.

***Figure 2. Key metrics evaluated by TCU***




*Source: Author's elaboration*

A further weakness was that only 4% of digital services (210 of 4,859) completed the quality self-diagnosis as per regulations[14]. SGD itself acknowledged that the instrument was not effective for comparative quality analysis' and announced a new Digital Service Maturity Index (IMDS); TCU maintained the finding while noting the initiative as mitigating context.

***Figure 3. Intended vs. Actual DPI Feedback Flow***

| Perpspective | Intended by Law | Actual State (TCU Audit Findings) |
|---|---|---|
| **Citizens** | Citizens rate services via Gov.br satisfaction API after each transaction. | API used by only ~25% of 4,859 services , with no free-text field and questions not service-specific. |
| **Service managers** | Service managers use API data to drive continuous improvement. | Zero of 4 audited managers cited the API as an improvement input. |
| **User** | User escalate seamlessly from rating to Fala.br complaint. | Re-authentication required and service not identifiable in 98.2% of Fala.br complaints. |
| **Advisory councils** | User advisory councils provide structured citizen voice. | Only 5% of services have councils and 83% have fewer than 9 members. |
| **Self-evaluation** | Self-diagnosis tool provides regular quality baseline. | Only 4% of services completed self-assessment and tool deemed ineffective by SGD. |

*Source: Author's elaboration*

[14] Ordinance SGD/ME 548/2022.

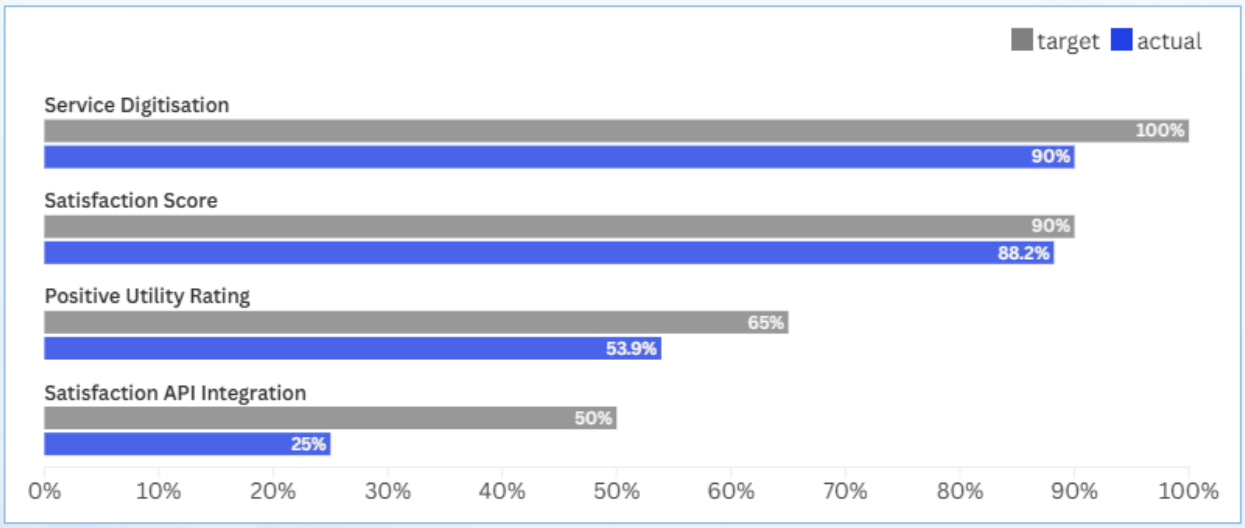
## 2. Absence of Performance Indicators and Non-Achievement of Digital Government Strategy Targets

The second finding addresses the transparency dimension of DPI governance. Brazil's Digital Government legislation[15] requires the federal monitoring dashboard to publish, for each service: the number of requests in progress and completed annually, average service delivery time, user satisfaction scores, and the number of simplification requests. TCU found that the first two (request volumes and average delivery time) were entirely absent from the dashboard, affecting transparency for approximately 87% of services (those with non-immediate delivery times).

The data gap is not merely cosmetic. As O'Reilly (2011) argues, data transparency is the mechanism through which digital government holds itself accountable: without published performance data, neither civil society nor oversight bodies can evaluate DPI effectiveness or hold service managers to account.

The DGS target[16] of connecting 50% of services to the satisfaction API by 2023 was also missed, with only 25%[17] integrated. The auditees, in response, cited legacy-system costs, competing priorities, managerial resistance to negative ratings, and technical incompatibilities. Three further DGS targets were near-misses: 90% service digitisation (target 100%), 4.41/5 satisfaction score (target 4.5), and 53.9% positive utility rating (target 65%), as shown in figure 4:

***Figure 4. DGS performance (actual versus targets)***




*Source: Author's elaboration*

In conclusion, the combined picture from both findings is of a DPI that has achieved impressive infrastructure scale but has not yet built the governance with proper feedback loops,

15 Law 14.129/2021 and Decree 8.936/2016.
16 Decree 10.332/2020, Initiative 2.1.
17 1,204 out of 4,859

performance accountability, and interoperability that would make it genuinely inclusive and continuously improving.

## Benchmarking Brazil's DPI Audit Against International Good Practice

To contextualise the TCU findings within global DPI governance standards, the audit results are benchmarked against three leading frameworks: the INTOSAI/ISSAI normative standards for IT audit and transparency; the OECD Digital Government Policy Framework; and the UK Government Digital Service (GDS) performance standards.

ISSAI 5300 requires auditors to assess whether IT systems have adequate performance monitoring and citizen accountability mechanisms (INTOSAI, 2019), and ISSAI 20 further requires public entities to make performance data accessible. The absence of request volumes and delivery times from Brazil's monitoring dashboard directly contravenes both standards.

The OECD Digital Government Policy Framework (OECD, 2020) identifies six maturity drivers — including *user-driven* and *data-driven* government, all of which Brazil's audit revealed as underperforming relative to its infrastructure level.

The UK Government Digital Service mandates publication of cost per transaction, satisfaction, completion rate, and digital take-up for every public-facing service (UK GDS, 2023) — exactly the indicators TCU found absent, demonstrating they are operationally achievable, not merely aspirational.

***Table 1. Benchmarking TCU Audit Findings Against International DPI Good Practice***

| Governance Dimension | International Best Practice (INTOSAI / OECD / UK GDS) | SAI Brazil Audit Finding |
|---|---|---|
| **Citizen feedback integration** | Mandatory satisfaction data with free-text comments linked to improvement plans (ISSAI 20 and UK GDS) | ▪ API only used by 25% of services<br>▪ No free-text field available<br>▪ not linked to improvement processes |
| **Performance transparency** | Cost per transaction, completion rate, delivery time published per service (UK GDS and OECD 2020) | ▪ Request volumes and delivery time absent from monitoring dashboard for ~87% of services |
| **Ombudsman interoperability** | Single point of escalation; automatic service identification; cross-level integration (OECD 2020) | ▪ *Fala.br* requires unneeded re-auth<br>▪ 98.2% of complaints not linked to a specific service<br>▪ Service is fragmented across federal/state/municipal levels |
| **Citizen participation in governance** | User panels with representative sampling; regular consultation cycles (ISSAI 5300) | ▪ 5% of services have user councils<br>▪ 83% of those have ≤9 members |

| Governance Dimension | International Best Practice (INTOSAI / OECD / UK GDS) | SAI Brazil Audit Finding |
|---|---|---|
| **Quality self-assessment** | Annual mandatory self-assessment with clear scoring rubric; results published (OECD and ISSAI 5300) | ▪ Only 4% completed<br>▪ Instrument acknowledged as ineffective<br>▪ IMDS still under development |
| **Strategic target accountability** | Published targets with annual progress reports; corrective action triggered on shortfall (OECD 2020) | ▪ DGS Initiative 2.1 missed by 25 pp<br>▪ No corrective plan in place at audit conclusion |

*Source: Author's elaboration.*

## Discussion: DPI Maturity and Inclusive Governance Gaps

The TCU audit findings, read together with international frameworks, reveal a characteristic pattern in emerging DPI ecosystems that can be termed as *infrastructure-ahead-of-governance*: substantial investments in the technical infrastructure of service delivery are not matched by commensurate investment in the accountability, transparency, and citizen-responsiveness mechanisms that determine whether that infrastructure truly serves all citizens equally.

This pattern has concrete equity consequences. Brazil's BPC[18] service received the lowest user satisfaction (3.64/5) of the four audited services, far below the simpler DEVIR (4.70/5). Focus groups described months-long waits, procedural dead-ends from undetected CadÚnico[19] data errors, and expensive travel for avoidable medical assessments. These are clearly governance failures, not technology failures, since the DPI lacked the feedback integration and proactive communication that would have prevented them, and in doing so amplified, rather than reduced, the disadvantages of the analogue service it replaced.

Accessibility compounds the picture: *Meu SUS Digital* and BPC had not completed required annual accessibility evaluations. For populations with limited digital literacy — who disproportionately depend on social services — inaccessible digital interfaces are exclusionary, directly undermining DPI's *leave no one behind* principle (UN, 2015).

The interoperability gap between *Fala.br* and *Gov.br* services illustrates how DPI components that are individually functional can fail to deliver value when the connective governance tissue is absent, what Janssen et al. (2012) identify as organisational and institutional barriers more than technical ones. In this case, SAI Brazil's recommended solution (SSO authentication, automatic data transfer and service-linked routing) is technically straightforward and the barrier elimination is an organisational prioritisation.

Encouragingly, the audit triggered immediate behavioural change. During the fieldwork phase, SGD updated the satisfaction API to add a free-text comment field and a direct link to *Fala.br*,

[18] disability social security for a highly vulnerable population.
[19] social program registration platform that identifies and characterizes low-income families.

registered by TCU as an effective benefit of the audit itself. This responsiveness demonstrates the catalytic value that SAI audits can have when DPI governance is the subject.

## Conclusion and SAI Audit Framework for DPI Governance

The TCU audit of Brazil's federal digital services offers the global SAI community a rich and replicable case study of DPI governance in a large, complex developing economy. Three headline lessons stand out.

First, infrastructure is necessary but not sufficient. Brazil's Level 3 DPI maturity has not yet been matched by feedback, accountability, and interoperability mechanisms required to translate infrastructure into inclusive service outcomes. This remains underdeveloped and SAIs should audit both: what exists and whether it works for citizens.

Second, the audit cycle itself is also a governance lever. The real-time improvements to the *Gov.br* satisfaction API triggered during TCU's fieldwork demonstrate that a credible audit presence accelerates DPI improvements. SAIs that audit DPI should expect and document these catalytic effects.

Third, the most vulnerable bear the highest cost of governance gaps, as seen in the BPC service's below-average satisfaction relative to simpler services, which reflects not technology gaps but a governance failure. Inclusive DPI governance requires SAIs to ask not just, *does it work?* but also *does it work for everyone?*

Based on the TCU audit and international frameworks reviewed, the following key elements of the audit domain are proposed in order to help other SAIs create and/or improve their Audit Frameworks for DPI Governance, where *capabilities* refer to direct delivery, experience, and user/customer-facing channel competencies; and *enablers*, on the other hand, refer to the structural infrastructure, governance, underlying technology, culture, and organizational processes that support these capabilities:

**Table 2**. Key elements proposed for SAI Audit Frameworks focused on DPI Governance

Capabilities Enablers

| Audit Dimension | Strategic Goal | What to Look For (examples) |
|---|---|---|
| **Feedback Coverage** | **Enhanced and customizable APIs**, featuring open-text fields for actionable feedback in the continuous improvement process. | What is the percentage of services connected to a citizen satisfaction mechanism? Is it service-specific, free-text enabled, and linked to improvement plans? |
| **Citizen Participation** | **Diversified evaluation and social participation models**, broadening civic engagement beyond the virtual platform | Do user advisory mechanisms exist at scale and represent actual users, including vulnerable populations? |

| Audit Dimension | Strategic Goal | What to Look For (examples) |
|---|---|---|
| **Performance Transparency** | **Full active transparency**, with automated publication of actual average response times and request abandonment rates. | Are mandatory performance indicators (request volumes, delivery times, satisfaction scores, simplification requests) publicly published per service? Is reporting current and consistent? |
| **Ombudsman Integration** | **Native interoperability with Single Sign-On (SSO)**, enabling automatic ticket creation with structured data fields. | Can citizens escalate from satisfaction rating to complaint in one step, with single sign-on (SSO) and automatic data transfer? |
| **Strategic Target Accountability** | **Detailed action plan backed by robust governance**, clear milestones, and deadlines to address resistance to user feedback. | Has the entity set quantitative DPI quality targets? Are these on track? If not, what corrective plans exist and are they adequately resourced? |
| **Equity and Accessibility** | **Enforcement of a Digital Service Maturity Index (IMDS)** and automated virtual queuing systems to guarantee fairness and legal rights. | Are services accessible to users with disabilities and limited digital literacy? Have previous accessibility audits (internal or external) been conducted? Is satisfaction data disaggregated by user vulnerability? |

*Source: Author's elaboration.*

The Brazilian case demonstrates that DPI audits add most value when they move beyond technical compliance to assess governance maturity — whether infrastructure is inclusive, whether citizens can influence it, and whether performance is transparent. Closing the gaps TCU identified requires not new infrastructure, but the will to make existing infrastructure accountable.

## References

Bannister, F. and Connolly, R. (2012) **Forward to the past: lessons for the future of e-government from the story so far**, Information Policy, 17(3–4), pp. 211–226.

Banga, K. and te Velde, D.W. (2021) **Digital public infrastructure and the data economy**. London: Overseas Development Institute.

Dempsey, M., Sherwood, E. and Ramasubramanian, R. (2022) **Governing digital public infrastructure**. London: Tony Blair Institute for Global Change.

G20 Digital Economy Working Group (2023) **G20 digital economy ministerial declaration**. New Delhi: Government of India.

Heeks, R. (2018) **Information and communication technology for development** (ICT4D). Abingdon: Routledge.

INTOSAI (2019): **Guidelines for IT audit**. Vienna: International Organisation of Supreme Audit Institutions.

INTOSAI WGITA (2022) **Guidance on auditing digital government**. Vienna: INTOSAI Working Group on IT Audit.

ITU and GIZ (2022) **GovStack implementation playbook**: building blocks for digital government. Geneva: International Telecommunication Union.

Janssen, M., Chun, S.A. and Gil-Garcia, J.R. (2012) **Building the next generation of digital government infrastructures**, Government Information Quarterly, 26(2), pp. 233–237.

Mergel, I., Edelmann, N. and Haug, N. (2019) **Defining digital transformation**: results from expert interviews, Government Information Quarterly, 36(4), 101385.

Ndou, V. (2004) **E-government for developing countries**: opportunities and challenges, The Electronic Journal on Information Systems in Developing Countries, 18(1), pp. 1–24.

O'Reilly, T. (2011) **Government as a platform**, Innovations: Technology, Governance, Globalization, 6(1), pp. 13–40.

OECD (2020) **The OECD digital government policy framework**: six dimensions of a digital government. Paris: OECD Publishing.

SGD (2024) **Digital Strategy of Federal Government 2024–2027**. Brasília, Brazil: Ministry of Management and Innovation in Public Services.

TCU (2024) **Quality of the Federal Government's Digital Public Services**. Audit Report in case number TC 002.007/2024-0. Federal Court of Accounts: Brasília, Brazil.

UK Government Digital Service (2023) **Service manual: measuring success** [online]. Available at: https://www.gov.uk/service-manual/measuring-success.

United Nations (2015) **Transforming our world: the 2030 agenda for sustainable development** (A/RES/70/1). New York: United Nations General Assembly.

United Nations Development Programme (2023) **Digital public infrastructure and the SDGs**. New York: UNDP.

# Digital Public Infrastructure as an Enabler for Inclusive Governance

**Malik Sulaiman Hamood Al Ghawi**
State Financial and Administrative
Audit Authority, Oman



## Abstract

Digital Public Infrastructure (DPI) refers to foundational, reusable digital platforms and building blocks such as digital identity, payments, and data exchange that underpin the development and delivery of trusted public and private services at scale. Properly governed DPI can improve inclusive governance by expanding access, increasing administrative transparency, improving efficiency, and creating reliable digital audit trails. This paper analyses DPI as a driver of inclusive governance, focusing on practical implementation experiences from Organisation for Economic Co-operation and Development (OECD) countries, European countries, Gulf countries, and Oman, together with audit and oversight methodologies, implementation challenges, lessons learned, and technical innovations relevant to Supreme Audit Institutions and public-sector IT auditors. It also addresses secure and partially isolated governance environments and proposes technical methods to verify that sensitive systems do not leak data beyond approved channels. The paper argues that DPI should be understood not only as a service-delivery stack but also as a public governance asset that requires strong legal, technical, and audit frameworks.

## Keywords

Digital Public Infrastructure; Inclusive Governance; Public Audit; Cybersecurity; Data Governance; Interoperability

## Introduction

The rapid growth of digital government has shifted public administration from isolated electronic services toward shared platforms and reusable building blocks that operate across sectors and institutions. These shared systems are increasingly described as Digital Public Infrastructure. Rather than focusing on one ministry or one application, DPI creates a national layer of capabilities that can be reused by multiple actors across the public and private sectors.

From a governance perspective, DPI matters because it can reduce service fragmentation, simplify citizen access, improve interoperability, support better policy delivery, and generate digital traces that strengthen accountability. At the same time, its scale and centrality create important risks relating to privacy, exclusion, concentration of power, cybersecurity, and operational resilience. For this reason, DPI must be understood as both a technological foundation and a governance arrangement.

## Conceptual Foundations of DPI

Recent international policy work commonly defines DPI as a set of shared, secure, and interoperable digital systems that enable broad access to public and private services. Core components usually include digital identification and authentication, digital payments, data exchange layers, trusted communication channels, and foundational government registries. These building blocks are normally supported by legal frameworks, institutional mandates, technical standards, and governance mechanisms that determine how they are used and controlled.

This conceptual model is important because DPI is not merely a collection of software platforms. It is a socio-technical infrastructure whose public value depends on the interaction between architecture, law, regulation, institutions, and oversight. A country may have strong technical systems but weak governance, or sound policy intentions but poor interoperability and implementation discipline. Inclusive governance therefore depends on how these layers work together.

## Practical Experiences with Digital Public Infrastructure

International experience shows that DPI creates the greatest public value when it is built as a reusable ecosystem rather than as isolated applications. Countries that have achieved sustainable progress in digital transformation generally rely on trusted digital identity, secure payment mechanisms, interoperable data exchange, and governance frameworks that enable multiple public institutions to deliver services through common digital foundations.

OECD and European approaches offer useful examples of this model. Several countries have built DPI on trusted digital identity, national registries, digital post systems, and structured interoperability frameworks. These platforms support tax administration, welfare services,

business processes, and healthcare interactions while relying on strong legal safeguards, institutional coordination, and standardized service architecture. Their experience demonstrates that long-term success depends less on isolated technical excellence than on governance maturity, institutional trust, and consistent implementation.

Countries across the Gulf region have also made significant progress in developing Digital Public Infrastructure. The United Arab Emirates has expanded digital identity and integrated government services across multiple sectors through unified digital platforms. Saudi Arabia has invested heavily in citizen-centred digital government initiatives that simplify service delivery while improving operational efficiency. Bahrain has strengthened interoperability frameworks and digital identity capabilities that support secure information exchange and improved administrative performance. Although implementation approaches differ, these experiences illustrate how coordinated governance, shared digital infrastructure, and strong institutional leadership can accelerate digital transformation.

Oman has likewise continued to strengthen its digital government capabilities through initiatives aligned with Oman Vision 2040. Continued investment in digital services, institutional modernization, and inter-agency integration has improved the foundations required for trusted digital service delivery. From a governance perspective, the Omani experience highlights that technology alone does not ensure successful transformation. Sustainable progress depends equally on effective governance, institutional accountability, cybersecurity, and continuous oversight that maintains public confidence while supporting innovation.

DPI has also played a major role in social protection and crisis response. Countries with usable identity and payment infrastructure were often better able to validate beneficiaries, deliver emergency support quickly, and reduce fraud or duplication. In this sense, DPI supports inclusive governance when it improves reach, reliability, administrative fairness, and resilience in the delivery of public value.

## Methodologies and Oversight Approaches

The audit of DPI requires a methodology that goes beyond conventional application review. Because DPI is cross-cutting and foundational, auditors should evaluate not only technology controls but also governance arrangements, legal authority, institutional accountability, and ecosystem-level risks. A robust audit approach should examine design, implementation, and operational effectiveness across identity, payments, data exchange, privacy, resilience, and service accountability.

In practice, this means combining compliance, performance, and IT audit perspectives. Auditors should test whether the legal framework adequately supports DPI, whether control ownership is clearly assigned, whether interoperability rules are applied consistently, and whether platform-level risks are monitored across all participating entities. Fieldwork should include

process walkthroughs, configuration review, access log testing, incident record analysis, sampling of transactions, and assessment of change management and resilience arrangements.

Continuous auditing is especially valuable in DPI environments because shared platforms generate high-volume, machine-readable evidence. Audit teams can use analytics to identify duplicate payments, suspicious authentication patterns, ghost beneficiaries, failed integration events, or unusual administrative access. Where governance is mature, these methods can support a shift from retrospective detection toward earlier and more preventive oversight.

## Implementation Challenges

Despite its promise, DPI presents major implementation challenges. The first is legal and institutional readiness. Effective DPI requires clear legal authority for identity, data sharing, privacy, electronic transactions, and service accountability, as well as cross-agency governance arrangements. If these arrangements are weak, digital integration may outpace trust, accountability, and public safeguards.

The second challenge is inclusion. Although DPI can simplify access, it may also exclude individuals who lack digital skills, reliable connectivity, language support, or suitable identification credentials. This means that inclusive governance depends on assisted channels, accessible design, and alternative service routes, especially for vulnerable groups.

The third challenge is technical complexity. DPI relies on interoperability, standardization, cybersecurity, master data quality, and resilience across many institutions. Legacy systems, fragmented ownership, inconsistent standards, and vendor lock-in can slow progress or increase risk. As integration deepens, so do the consequences of systemic failures.

## Secure and Isolated Governance

In some public-sector environments, governance must support systems that are partially disconnected from the Internet or logically isolated from external networks. This is especially relevant in critical infrastructure, national security, highly sensitive population databases, and core fiscal or operational environments. In such cases, the governance challenge is not only how to provide digital services, but how to do so without exposing sensitive systems to uncontrolled external connectivity.

However, isolation by itself is not a complete security strategy. Sensitive data can still leak through removable media, insider misuse, weak export controls, or covert technical channels. Therefore, air-gapped or logically isolated DPI environments should combine physical or logical separation with zero-trust principles inside the enclave. These include least privilege, strong administrator authentication, endpoint restrictions, monitored staging zones, immutable logs, and tightly governed data export procedures.

A sound governance model for isolated infrastructure includes data classification tied to export rules, multi-party approval for bulk extraction, DLP-style monitoring of copying and removable media, and periodic testing to verify that no unauthorized path exists for data exfiltration. In this model, secure governance is not assumed from separation alone; it is demonstrated through measurable controls and repeated verification.

## Technical Assurance and Leakage Testing

To confirm that a sensitive system does not leak data, governance controls must be supported by technical assurance procedures. The first layer is configuration verification. Auditors should inspect firewall rules, routing paths, endpoint control policies, Domain Name System (DNS) behavior, USB restrictions, administrative access settings, and controlled-transfer gateway configurations. The goal is to confirm that only explicitly approved communication paths exist.

The second layer is log-based verification. Auditors should correlate operating-system logs, file integrity alerts, database audit trails, privileged-access records, DLP events, and transfer gateway logs to identify unusual extraction behavior. Large data pulls, repeated compression of sensitive files, after-hours copying, and abnormal use of administrative tools should all be treated as indicators for deeper review.

The third layer is controlled adversarial testing. Internal security teams or trusted assurance units should attempt to exfiltrate non-sensitive test data using realistic techniques such as USB storage, staged archives, unauthorized scripts, or hidden scheduled tasks. The objective is to prove that detective and preventive controls work in practice, rather than only appearing adequate in policy or architecture diagrams.

## Illustrative Technical Application

The following SQL query helps identify unusually large data-extraction operations from a sensitive table:

```
SELECT user_id, DATE(event_time) AS day, COUNT(*) AS extract_count, SUM(rows_returned) AS total_rows
FROM db_query_audit
WHERE object_name = 'citizen_master'
AND action_type = 'SELECT'
GROUP BY user_id, DATE(event_time)
HAVING SUM(rows_returned) > 50000
ORDER BY total_rows DESC;
```

This query can be calibrated to local norms and used to detect excessive data access, bulk downloads, or possible misuse of records.

The following Python example highlights suspicious file copies to removable media using endpoint logs:

```
import pandas as pd

import re

logs = pd.read_csv('endpoint_file_events.csv')
usb_paths = ['/media/', 'E:\\', 'F:\\']
pattern = '|'.join(map(re.escape, usb_paths))

suspect = logs[
   logs['destination_path'].str.contains(pattern, case=False, na=False) &
   (logs['bytes_written'] > 10000000)]

result = suspect.groupby(['user','destination_path']).agg

   (events=('event_id','count'),
   bytes_total=('bytes_written','sum')
   ).reset_index()
```

In operational environments, this logic should be integrated into centralized monitoring or SIEM workflows and linked to approval tickets, identity context, and incident management.

## Lessons Learned and Innovation

Several lessons emerge from global DPI experience. First, modular and reusable building blocks create greater long-term value than isolated digital projects. Second, governance quality determines whether DPI builds trust or merely expands technical dependence. Third, audit and control functions must evolve from document-driven review toward analytics-enabled, architecture-aware, and preventive assurance models.

Innovation in this area increasingly focuses on privacy-preserving interoperability, open standards, digital commons governance, anomaly detection, and continuous monitoring. For public auditors, the most significant implication is the opportunity to move from ex post review toward earlier risk detection using system telemetry, transaction analytics, and structured technical testing.

## Conclusion

Digital Public Infrastructure can be a powerful enabler of inclusive governance when it is secure, interoperable, auditable, and rights-aware. It can improve service reach, reduce fragmentation, strengthen administrative consistency, and generate the evidence needed for more effective oversight. Yet these benefits are not automatic; they depend on strong governance design, legal safeguards, technical discipline, and institutional capability.

Governments and oversight bodies should therefore treat DPI as both strategic infrastructure and a permanent audit domain. The most resilient model is one that combines service convenience with controlled data exchange, measurable security controls, and rigorous verification that sensitive systems do not leak information.

## References


Communications of the ACM. (2023). *Bridgeware: The Air-Gap Malware*. https://cacm.acm.org/research/bridgeware/

GovTech Singapore. (n.d.). *Data Loss Prevention*. https://www.tech.gov.sg/products-and-services/for-government-agencies/ict-and-infrastructure/data-loss-prevention/

OECD. (2024). *Digital Public Infrastructure for Digital Governments*. https://www.oecd.org/en/publications/digital-public-infrastructure-for-digital-governments_ff525dc8-en.html

United Nations Development Programme (UNDP). (2023). *Accelerating the SDGs through Digital Public Infrastructure*. https://www.undp.org/

World Bank. (2023). *Digital Public Infrastructure (DPI) Thinking*. https://thedocs.worldbank.org/

ArXiv. (2023). *Mind the Gap: Can Air-Gaps Keep Your Private Data Secure?* https://arxiv.org/html/2409.04190v1

# Auditing Digital Public Infrastructure During Implementation: Lessons from Brazil's Gestão Presente System (SGP)

Klauss Nogueira,
Fernando Faria,









Harley Ferreira &
Rafael Albuquerque
Federal Court of Accounts, Brazil

## 1. Introduction

Digital Public Infrastructure (DPI) is playing an increasingly important role in governments' digital transformation efforts (G20 India Presidency, 2023). Built on shared data platforms, interoperability mechanisms, and integrated digital services, DPIs enable public institutions to collaborate in the implementation of public policies and the delivery of services to citizens.

In recent years, countries around the world have invested in national data infrastructures to support sectors such as education, healthcare, social assistance, and social protection. While these initiatives offer significant opportunities to improve government efficiency and generate public value, they also introduce new challenges related to data governance, institutional coordination, technological sustainability, and risk management.

In this context, Supreme Audit Institutions (SAIs) face an additional challenge: how to oversee large-scale digital platforms that are still under development and whose risks may materialize

before full implementation. For initiatives of this nature, traditional audits conducted after systems become operational do not always provide the best opportunities for prevention and governance improvement.

This article presents the experience of the Brazilian Federal Court of Accounts (TCU) in monitoring the implementation of the Gestão Presente System (SGP), a national basic education data platform developed by Brazil's Ministry of Education. Designed to integrate information from federal, state, district, and municipal education networks, the platform supports the monitoring of students' educational trajectories and provides information to guide policies aimed at improving school retention and educational outcomes.

Rather than simply describing a specific oversight engagement, this article seeks to share lessons learned from auditing Digital Public Infrastructure during implementation. The TCU experience demonstrates how preventive and risk-based approaches can contribute to stronger governance, improved data quality, and greater effectiveness of public policies supported by digital platforms.

## 2. The Gestão Presente System: A Digital Public Infrastructure for Education

The digital transformation of the public sector has accelerated the development of national platforms designed to integrate data and support public policymaking. Commonly classified as Digital Public Infrastructure (DPI), these initiatives provide shared capabilities that can be used by multiple government entities and programs.

In Brazil, a recent example is the Gestão Presente System (SGP), developed by the Ministry of Education (MEC) as a national platform for the integration and management of basic education data. The system was designed to consolidate information from federal, state, district, and municipal education networks, providing greater visibility into students' educational trajectories and supporting the implementation of education policies.

In addition to consolidating academic and administrative information, SGP seeks to strengthen the monitoring and management capabilities of education authorities by providing more timely and reliable information for public managers. The initiative also supports programs aimed at improving school retention and reducing dropout rates, reinforcing the strategic role of data in the design and monitoring of public policies.

From a digital governance perspective, SGP displays the core characteristics of a Digital Public Infrastructure. Its effectiveness depends on the integration of multiple systems, the quality of shared data, cooperation among different levels of government, and the existence of appropriate governance, security, and technological sustainability mechanisms.

These characteristics make the platform particularly relevant for Supreme Audit Institutions (SAIs). Unlike systems used by a single organization, national data platforms tend to concentrate critical information and support multiple public policies simultaneously. As a result, weaknesses

in their design or governance may generate amplified impacts, affecting both the reliability of information and the effectiveness of the government actions that depend on it.

By bringing together strategic information for educational management and supporting nationwide public policies, the Gestão Presente System represents a relevant example of both the opportunities and the challenges associated with implementing Digital Public Infrastructure. These characteristics motivated the oversight engagement discussed in the following section.

## 3. Auditing a Digital Public Infrastructure During Implementation

The characteristics of the Gestão Presente System (SGP) posed specific challenges for external oversight. As a Digital Public Infrastructure still under implementation, weaknesses related to governance, data quality, institutional coordination, or technological sustainability could compromise the platform's effectiveness before it reached full operational maturity.

In light of this context, the Brazilian Federal Court of Accounts (TCU) decided to conduct an oversight engagement during the implementation phase, focusing on the early identification of risks that could affect the initiative's future outcomes. The objective was to create opportunities to strengthen governance before potential issues materialized into operational failures or negatively affected the public policies supported by the platform.

The engagement was conducted through a Monitoring Report (Relatório de Acompanhamento – RACOM), a TCU oversight instrument used to monitor initiatives under development and assess risks throughout their implementation. This approach proved particularly suitable for a digital infrastructure still in the process of consolidation, allowing the audit team to follow the project's evolution and maintain continuous dialogue with responsible managers.

Rather than concentrating efforts on retrospective compliance verification, the team adopted a risk-based approach. The objective was to identify the factors most critical to the success of the initiative, assess their potential impacts, and evaluate whether adequate mitigation measures were in place.

As part of this process, the team developed a risk matrix covering issues related to data governance, auditability, intergovernmental coordination, technological sustainability, and contract governance. The matrix was subsequently shared with the managers responsible for the initiative, who provided their assessments and described the measures planned to address the identified risks.

This process resulted in a strongly preventive oversight approach. Instead of merely identifying weaknesses, the audit sought to understand how risks were being managed and whether appropriate controls and mitigation measures had been established. The dialogue with managers enabled the team to assess not only the existence of risks but also the institutional capacity required to address them.

Another important aspect of the approach was the incorporation of the perspectives of the platform's institutional users. Since the success of SGP depends on the active participation of state and municipal education networks, the audit team considered it essential to understand how potential users perceived the initiative. To achieve this, consultations were conducted with State Departments of Education, with the support of the National Council of State Education Secretaries (Consed), allowing the team to identify challenges related to system adoption, data integration, and intergovernmental governance.

The experience demonstrated that auditing Digital Public Infrastructure requires a broader perspective than that traditionally applied to conventional information technology projects. Technical aspects remain important, but their effectiveness depends on the interaction of institutional, regulatory, and organizational factors. In national data platforms, issues related to governance, stakeholder coordination, and information quality can be just as important as the technology itself.

The main stages of the oversight approach adopted by TCU are summarized in Table 1.

**Table 1 – Main Stages of the Oversight Approach Adopted by TCU**

| Oversight Stage | Purpose |
|---|---|
| Continuous monitoring (RACOM) | Monitor the implementation of the digital infrastructure throughout its development |
| Risk Assessment | Identify factors that could compromise the success of the initiative |
| Dialogue with managers | Understand existing controls and planned mitigation measures |
| User consultation (Consed) | Incorporate the perspectives of the platform's main institutional users |
| Recommendations and improvements | Strengthen governance and reduce the likelihood of risk materialization |

**Source:** Prepared by the authors based on the oversight of the Gestão Presente System.

At the conclusion of the initial monitoring phase, the primary outcome was not the identification of irregularities that had already occurred, but the development of a structured understanding of the risks associated with the platform's implementation and the measures needed to address them. The experience demonstrated the potential of continuous monitoring engagements to strengthen the governance of Digital Public Infrastructure before it reaches full operational maturity.

## 4. Key Challenges Identified During the Audit

The oversight of the Gestão Presente System identified challenges that are not unique to the education sector or the Brazilian context. Many of them are common to Digital Public Infrastructure initiatives that seek to integrate data, institutions, and processes at scale.

The experience demonstrated that the success of such platforms depends not only on appropriate technological solutions, but also on robust governance arrangements, institutional coordination, and effective risk management practices.

### 4.1 Ensuring Data Quality and Reliability

The first set of challenges was related to data governance and data quality. Like any infrastructure built on information sharing, the value generated by the system depends directly on the reliability of the records received from different education networks.

The audit highlighted the need to strengthen governance mechanisms capable of ensuring the consistency, integrity, and timeliness of the information processed by the platform. In environments where multiple organizations produce and share data, clearly defined responsibilities and controls are essential to ensure that information can be safely used for policymaking and performance monitoring.

### 4.2 Ensuring Transparency and Traceability

Another challenge concerned the ability to trace the origin, modifications, and processing flows of the information managed by the platform.

In Digital Public Infrastructure initiatives, auditability is a fundamental requirement for ensuring transparency, accountability, and institutional trust. The absence of adequate traceability mechanisms may hinder the identification of inconsistencies, compromise verification processes, and reduce confidence in the information used by public managers.

The experience reinforced the importance of incorporating auditability requirements from the earliest stages of infrastructure development, avoiding the need for costly retrofitting at later stages.

### 4.3 Promoting Coordination and User Engagement

The success of a national platform depends not only on the technology employed, but also on the level of engagement and participation of the organizations responsible for supplying and using the data.

In this context, the audit highlighted the importance of coordination among different levels of government and the establishment of permanent mechanisms for institutional cooperation.

Consultations with State Departments of Education revealed that factors such as user support, system integration, and communication play a significant role in the effective adoption of the platform.

The experience demonstrated that Digital Public Infrastructure initiatives are simultaneously technology projects and institutional coordination projects.

## 4.4 Ensuring Technological Sustainability

The oversight engagement also examined issues related to the technological sustainability of the solution.

In large-scale platforms, architectural decisions made during implementation can have long-term consequences, influencing costs, operational flexibility, and the infrastructure's ability to evolve over time.

Accordingly, the audit assessed whether risks related to technological dependence, operational continuity, and future evolution of the platform were being adequately considered by managers. Rather than focusing on specific technologies, the primary concern was whether appropriate mechanisms existed to ensure the long-term sustainability of the initiative.

## 4.5 Strengthening Contract Governance

Finally, the audit highlighted the importance of contract governance for the success of Digital Public Infrastructure initiatives.

Projects of this nature typically involve multiple suppliers, specialized services, and long-term contractual arrangements. The effectiveness of the platform depends not only on the technical quality of the contracted solutions, but also on the existence of appropriate mechanisms for monitoring performance, overseeing contract execution, and managing risks.

The experience demonstrated that contracts and technology cannot be analyzed in isolation. In digital transformation initiatives, contract governance forms an integral part of the governance of the Digital Public Infrastructure itself.

# 5. Lessons Learned and Recommendations

The experience of monitoring the Gestão Presente System generated lessons that may be useful for other Supreme Audit Institutions (SAIs) involved in auditing Digital Public Infrastructure. Although national contexts vary, many of the challenges identified during the oversight engagement are likely to recur in similar initiatives.

## Lesson 1: Audit the Infrastructure Before It Becomes Critical

In traditional projects, audits are often conducted after systems have already been implemented. In the case of Digital Public Infrastructure, this approach may significantly reduce opportunities for prevention.

The TCU experience demonstrated that monitoring during the implementation phase makes it possible to identify structural risks at a stage when corrective actions can still be adopted more efficiently. The more integrated and strategically important an infrastructure becomes, the more complex and costly it is to address governance, architectural, or data quality issues.

## Lesson 2: Evaluate Governance, Not Just Technology

Digital Public Infrastructure initiatives are often perceived primarily as technology projects. However, the audit revealed that many of the most significant risks were related to governance arrangements, the definition of responsibilities, and institutional coordination mechanisms.

Issues such as decision-making processes, data governance, accountability, and collaboration among organizations can be just as important to the success of an initiative as the quality of the technological solution itself.

## Lesson 3: Prioritize the Most Relevant Risks

Digital Public Infrastructure initiatives are dynamic environments that evolve rapidly during implementation. In such contexts, traditional approaches based exclusively on ex-post assessments may limit opportunities for prevention and reduce the usefulness of audit recommendations.

The TCU experience demonstrated the benefits of combining continuous monitoring with structured risk analysis. This approach enabled the audit team to focus its efforts on the factors most critical to the success of the initiative, foster dialogue with managers, and monitor the implementation of mitigation measures before risks materialized.

## Lesson 4: Listen to Infrastructure Users

The performance of a Digital Public Infrastructure depends not only on its developers or central managers. Its success is directly linked to the experience of the users responsible for providing, maintaining, and utilizing the information processed by the platform.

Consultations with State Departments of Education provided insights that would have been difficult to obtain through document analysis alone. The experience reinforced the importance of incorporating users' perspectives into evaluations conducted by Supreme Audit Institutions.

### Lesson 5: Treat Data as a Strategic Asset

The most valuable asset of a Digital Public Infrastructure is not the software, the technological infrastructure, or the associated contracts. Its greatest asset is the data that supports public policies, decision-making processes, and services delivered to society.

For this reason, issues related to data quality, integrity, traceability, and governance should occupy a central place in audits. The reliability of the information produced by a platform directly influences its ability to generate public value.

### Recommendations for Supreme Audit Institutions

Based on this experience, Supreme Audit Institutions should consider adopting preventive and risk-based approaches when auditing Digital Public Infrastructure. Audits conducted during implementation can contribute to stronger governance, improved data quality, and greater effectiveness of the public policies supported by these platforms.

As governments expand the use of integrated data systems and digital services, the importance of audit models capable of assessing not only compliance, but also the ability of technological solutions to generate public value in a sustainable, transparent, and trustworthy manner will continue to grow.

## 6. Next Steps

The experience of monitoring the Gestão Presente System provided an important learning opportunity for the Brazilian Federal Court of Accounts (TCU) regarding the challenges associated with auditing Digital Public Infrastructure. The engagement demonstrated that national data platforms require oversight approaches that combine expertise in technology, governance, risk management, and public policy evaluation.

As governments continue to expand the use of Digital Public Infrastructure in areas such as education, healthcare, social assistance, and public service delivery, the need for oversight models capable of acting preventively and monitoring initiatives during implementation is likely to increase.

In this context, the Gestão Presente experience reinforced the importance of continuous monitoring mechanisms, risk-based assessments, and processes that incorporate the perspectives of platform users. These approaches can enhance the ability of Supreme Audit Institutions (SAIs) to identify vulnerabilities at an early stage and contribute to strengthening governance before problems materialize.

For TCU, the engagement also provided an opportunity to refine practices that may be applied to future audits of Digital Public Infrastructure. The growing integration of data, digital platforms,

and public policies suggests that initiatives of this nature will become increasingly common in the years ahead, requiring oversight methods capable of evaluating not only technological aspects, but also public value generation, data quality, and the long-term sustainability of digital solutions.

The experience described in this article suggests that preventive and risk-based audits can make a significant contribution to the success of Digital Public Infrastructure initiatives, strengthening their ability to support public policies and deliver lasting benefits to society.

## 7. Conclusion

The expansion of Digital Public Infrastructure is transforming the way governments design, implement, and monitor public policies. By integrating data, institutions, and services at scale, these platforms increase the potential for public value creation while also introducing new challenges related to governance, information quality, and institutional sustainability.

The experience of the Brazilian Federal Court of Accounts (TCU) in monitoring the implementation of the Gestão Presente System demonstrated that auditing Digital Public Infrastructure requires approaches that differ from those traditionally applied to information technology projects. Rather than focusing solely on technical components, auditors must also examine data governance, stakeholder coordination, risk management, and the initiative's ability to sustainably support public policies over time.

The use of a preventive and risk-based approach enabled the identification of significant challenges while the platform was still under implementation, creating opportunities to strengthen governance and improve oversight mechanisms before problems materialized. The experience also highlighted the importance of incorporating users' perspectives and treating data as a strategic asset for generating public value.

As Digital Public Infrastructure becomes an essential component of public service delivery and policy implementation, the role of Supreme Audit Institutions (SAIs) in promoting effectiveness, transparency, and sustainability becomes increasingly important. The case of the Gestão Presente System suggests that audits conducted during implementation can generate substantial benefits by enabling the timely identification of risks and strengthening governance before weaknesses evolve into structural problems.

The main lesson from this experience is straightforward: the more strategic a digital infrastructure is for the implementation of public policies, the greater the benefit of auditing it before it becomes indispensable.

## References

Brazil. Federal Court of Accounts (TCU). Monitoring of the Gestão Presente System.

Judgment 949/2026-Plenary. Brasília, Brazil, 2026.

Available at:

https://portal.tcu.gov.br/uploads/noticias/pdf/2026/04/15/AAA_008.418-2025-0-_AAA-_ACOM.pdf.

Accessed June 15, 2026.

Brazil. Ministry of Education (MEC). Gestão Presente System.

Available at:

https://www.gov.br/mec/pt-br/mec-gestao-presente/sistema-gestao-presente.

Accessed June 15, 2026.

G20 India Presidency. A Framework for Digital Public Infrastructure.

New Delhi, India, 2023.

Available at:

https://www.g20.org/content/dam/gtwenty/gtwenty_new/document/G20%20Framework%20for%20Systems%20of%20Digital%20Public%20Infrastructure.pdf.

Accessed June 15, 2026.



Section VI

# COUNTRY JOURNEYS: BUILDING DPI IN EMERGING ENVIRONMENTS

# Digital Public Infrastructure as an Enabler of Inclusive Governance: An Audit Perspective from Sierra Leone


## Abu Allicious Gogra-Hilton

Audit Service Sierra Leone





## Abstract

Digital Public Infrastructure (DPI) has emerged as a transformative governance architecture, providing shared digital foundations encompassing digital identity systems, interoperable payment rails, and data exchange platforms that enable governments to deliver services equitably and efficiently. This article examines DPI as an enabler of inclusive governance through an audit lens, with particular reference to Sierra Leone and its Supreme Audit Institution, the Audit Service Sierra Leone (ASSL). Drawing on international DPI governance practices across India, the European Union, and select AFROSAI-E member states, the article argues that the full governance potential of DPI can only be realized when accompanied by robust Information Systems (IS) audit oversight aligned with INTOSAI's ISSAI 5300 and COBIT 2019 frameworks. Sierra Leone's nascent DPI landscape, anchored by the biometric National Identification System and the Bank of Sierra Leone's mobile money interoperability framework presents significant opportunities for inclusive service delivery but is constrained by limited IS audit capacity within ASSL. This article proposes a DPI Audit Maturity Model (DPI-AMM) for low- and middle-income countries, structured around four dimensions: digital identity integrity, payment system reliability, data governance, and equity-focused performance. It concludes with targeted recommendations for ASSL and AFROSAI-E member institutions, underscoring the critical role of IS audit in ensuring that DPI serves as a public good rather than an instrument of exclusion or misappropriation.

## Keywords

*Digital Public Infrastructure, Inclusive Governance, IS Audit, ISSAI 5300, Sierra Leone, Supreme Audit Institutions*

## 1. Introduction

Digital Public Infrastructure (DPI) refers to the shared, open digital systems that underpin modern governance and economic participation. Distinguished from proprietary digital services, DPI is characterized by its public-good orientation: open standards, interoperability, and equitable access. The archetypal DPI stack comprises three foundational layers: digital identity, enabling citizens to authenticate and transact; payment infrastructure, enabling universal financial participation; and data exchange platforms, enabling consent-based information sharing across sectors.

The governance significance of DPI has gained momentum through global policy frameworks. The G20 New Delhi Declaration (2023) endorsed DPI as a strategic enabler of the Sustainable Development Goals (SDGs), particularly SDG 16 (Peace, Justice and Strong Institutions) and SDG 9 (Industry, Innovation and Infrastructure). The United Nations Secretary-General's Roadmap for Digital Cooperation (2020) similarly identified DPI as foundational to inclusive digital transformation, recognizing that access to digital identity, financial services, and government information is a precondition for meaningful civic participation.

For Supreme Audit Institutions (SAIs), DPI presents a dual imperative. First, SAIs can leverage DPI-enabled data ecosystems for more evidence-based, real-time public expenditure audits. Second, and more critically, SAIs must exercise independent oversight of DPI systems themselves by assessing procurement integrity, technical governance, and equity outcomes. Sierra Leone's context makes this imperative especially pressing. As the Audit Service Sierra Leone (ASSL) navigates the country's emerging digital governance landscape, the absence of a dedicated IS audit framework for DPI creates a structural accountability gap that this article seeks to address.

## 2. Understanding DPI in the Governance Context

DPI is most effectively conceptualized through the three-layer stack framework endorsed by the G20 Digital Economy Working Group and the Centre for Digital Public Infrastructure (CDPI). When developed as genuine public goods governed by open standards, maintained as shared infrastructure, and subject to independent oversight, these three layers create the structural conditions for inclusive governance, as illustrated in Figure 1:

- **Digital Identity:** Unique, verifiable identification systems, biometric national IDs, digital credentials allowing citizens to authenticate their identity across public and private services, enabling access to welfare, health, and legal processes.

- **Payment Infrastructure:** Interoperable, real-time payment systems such as mobile money rails, central bank digital payment gateways enabling universal financial participation and facilitating direct-benefit transfers to eligible citizens.
- **Data Exchange Platforms:** Consent-based, API-enabled data-sharing protocols allowing government and private-sector actors to share citizen data securely and transparently, reducing administrative redundancy and improving service coordination.

When these layers are governed as public goods, citizens can access healthcare, education, and social protection without physical intermediaries. Governments can identify and eliminate ghost beneficiaries in public payroll and social transfer programs. The inclusivity potential of DPI, however, depends critically on the governance quality of these systems their —security, accessibility, interoperability, and accountability to citizens.




**Figure 1:** The DPI Three-Layer Governance Stack

*Source: Author's own compilation based on CDPI (2023) and G20 New Delhi Declaration (2023)*

## 3. The Audit Imperative: Why DPI Demands SAI Oversight

DPI introduces governance risks that are qualitatively different from those addressed by conventional financial audits. Four risk categories are especially significant for SAIs, as summarized in Table 2 (DPI Governance Risk Register):

**a) Data Governance and Privacy Risks:** DPI systems aggregate personal, biometric, and financial data at scale. Without robust data governance frameworks, these systems can be weaponized for surveillance, algorithmic discrimination, or corruption. SAIs must assess whether DPI data controllers have implemented appropriate data protection measures, consent mechanisms, and breach notification protocols.

**b) Procurement and Implementation Integrity:** Large-scale DPI deployments involve complex, multi-year procurement processes susceptible to irregularities. The selection of DPI vendors, structuring of contracts, and management of implementation milestones fall squarely within the SAI audit mandate.

**c) Interoperability and Technical Standards:** DPI built on proprietary, vendor-specific platforms creates long-term lock-in risks threatening fiscal sustainability and service continuity. SAIs should assess whether DPI systems comply with open interoperability standards and whether contractual exit provisions are adequately protected.

**d) Equity and Inclusion Performance:** DPI that excludes women, rural populations, elderly citizens, or persons with disabilities fails its fundamental governance promise. Performance audits of DPI must incorporate equity metrics: penetration rates by demographic group, accessibility compliance, and remediation mechanisms for excluded populations.

ISSAI 5300 — the INTOSAI standard governing IS audit provides the overarching normative framework for SAIs engaging with DPI. Complementary guidance is available through COBIT 2019's governance objectives, particularly those addressing alignment, planning, and organization (APO) in digital service delivery environments (ISACA, 2018; INTOSAI, 2016).

**Table 2: DPI Governance Risk Register for Supreme Audit Institutions**

| Risk Category | DPI Component | Risk Description | Likelihood | Impact | SAI Audit Response |
|---|---|---|---|---|---|
| **Data Governance** | All layers | Unauthorized access, data breach or misuse of citizen data | High | Very High | IS Security & Privacy Audit |
| **Procurement** | Payment infrastructure | Vendor lock-in; contract irregularities in DPI procurement | Medium | High | Compliance & Contract Audit |
| **Technical** | Digital identity | Biometric system failure or enrolment exclusion errors | Medium | High | Systems Reliability Audit |
| **Equity** | All layers | Digital exclusion of rural, elderly and marginalized groups | High | High | Performance Audit |

| Risk Category | DPI Component | Risk Description | Likelihood | Impact | SAI Audit Response |
|---|---|---|---|---|---|
| **Financial** | Payment infrastructure | Transaction fraud and undetected public revenue leakage | Medium | High | Forensic Audit |
| **Operational** | Data exchange | System downtime or interoperability failures disrupting services | Low | High | Business Continuity Audit |

*Source: Author's compilation based on ISSAI 5300, COBIT 2019, and INTOSAI WGITA guidance*

## 4. Sierra Leone's DPI Landscape: Emerging Architecture, Persistent Gaps

Sierra Leone has made incremental but meaningful progress in digital infrastructure. The National Civil Registration Authority (NCRA) has established a biometric national identification system known as the Sierra Leone ID (SL-ID), constituting the embryonic digital identity layer of a nascent DPI stack. The Bank of Sierra Leone (BSL) has issued mobile money interoperability regulations laying the foundations for unified digital payment rails. The Sierra Leone Digital Transformation Project (SLDTP), established under the Ministry of Communication, Technology, and Innovation, signals government's commitment to a coherent national digital strategy.

However, critical structural gaps persist. Such as, there is no unified data exchange protocol linking government ministries, departments, and agencies (MDAs). Digital identity coverage remains low, with significant exclusion in the southern and eastern provinces. Cybersecurity frameworks are nascent, with no designated government Computer Emergency Response Team (CERT). Most critically, the ASSL has not yet developed a dedicated IS audit methodology for DPI, creating an accountability vacuum precisely as digital infrastructure expands (Audit Service Sierra Leone, 2023).

This gap is not unique to Sierra Leone. As illustrated in Figure 2 below, a 2022 AFROSAI-E survey of member SAIs found that fewer than 30% had conducted IS audits of national identity or payment systems in the preceding three years, and fewer than 15% had a dedicated IS audit unit with certified practitioners. The challenge is both technical and institutional, requiring a systemic response at the national and regional levels (AFROSAI-E, 2022).

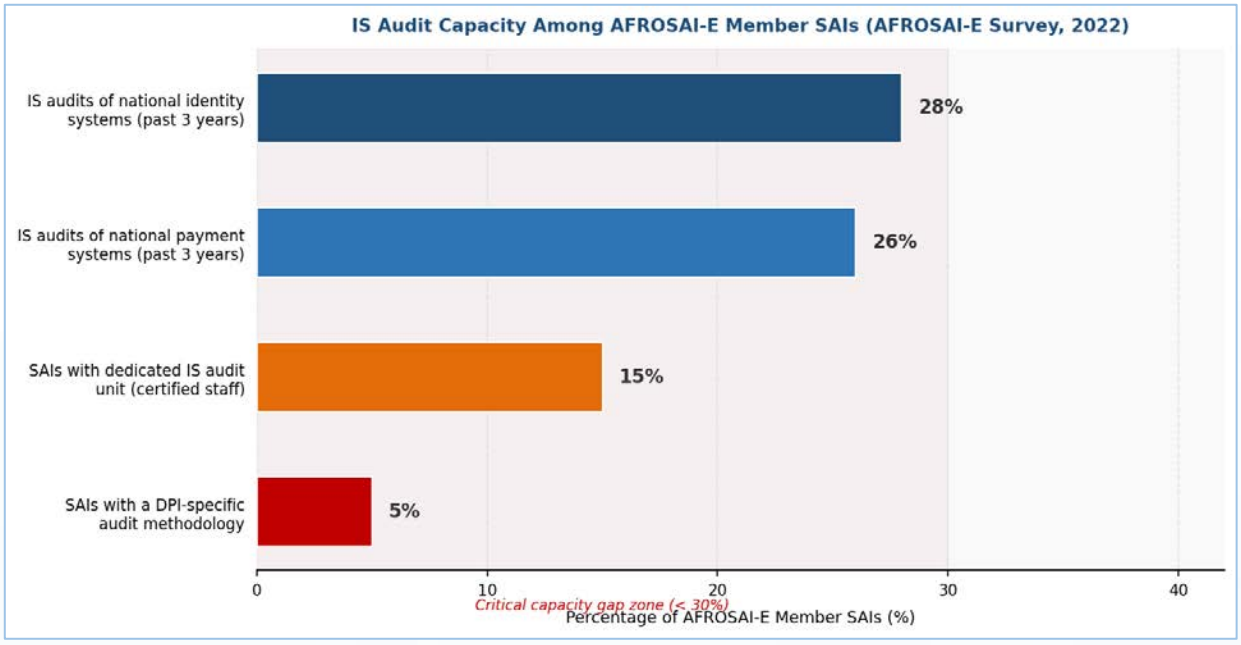



**Figure 2:** IS Audit Capacity Among AFROSAI-E Member SAIs

*Source: AFROSAI-E Survey (2022); Author's compilation*

## 5. International DPI Governance Practices: Benchmarks for SAI Oversight

A review of international DPI deployments yields governance benchmarks directly relevant to ASSL and comparable AFROSAI-E member SAIs. Three cases — India, the European Union, and selected African states illuminate the audit challenges and institutional responses that accompany large-scale DPI deployments.

**India's India Stack:** India's DPI architecture, comprising of Aadhaar (biometric identity with over 1.3 billion enrolments), the Unified Payments Interface (UPI), and the Data Empowerment and Protection Architecture (DEPA) constitutes the world's most extensive DPI deployment. India's Comptroller and Auditor General (CAG) has confronted the challenge of auditing DPI systems at an unprecedented scale, surfacing concerns around biometric data security, exclusion errors in social benefit transfers, and algorithmic discrimination risks. The India Stack experience demonstrates that DPI scale amplifies audit complexity: as more public services are mediated through DPI, the accountability stakes for SAIs increase proportionally (World Bank, 2022; CDPI, 2023).

**The European Union's eIDAS 2.0 Framework:** The EU's revised regulation on electronic identification and trust services (eIDAS 2.0, 2024) offers a contrasting model built on privacy-by-design and federated governance. The framework mandates that digital identity wallets meet accessibility standards, data minimization requirements, and cross-border interoperability, each constituting an auditable governance commitment. The European Court of Auditors (ECA) has provided guidance on auditing digital transformation programs, emphasizing that SAIs must

assess not only technical compliance but also the equity of digital service outcomes for marginalized populations (European Commission, 2024).

**African Precedents — Rwanda and Ghana:** Within Africa, Rwanda's Irembo platform and Ghana's National Identification System (Ghana Card) offer contextually proximate examples for Sierra Leone. Rwanda's Irembo; a digital services portal anchored to a biometric identity layer adopted an incremental deployment model with IS audit gates built into each implementation phase. The Office of the Auditor General of Rwanda progressively developed IS audit capabilities alongside DPI expansion. In Ghana, the Auditor-General has initiated IS audits of the National Identification Authority (NIA), providing a directly applicable precedent for ASSL's IS audit development agenda (AFROSAI-E, 2022).

Three overarching lessons emerge from this international survey, each directly actionable for ASSL:

**Rights-by-design auditing:** SAIs in jurisdictions, such as the EU, audit DPI not merely for technical compliance but for adherence to privacy-by-design and equity-by-design principles. Adopting this standard, which aligns with ISSAI 5300's performance audit guidance would position ASSL to provide more substantive assurance over Sierra Leone's emerging DPI ecosystem.

**Federated oversight coordination:** Effective DPI governance requires structured coordination across multiple regulatory bodies like data protection authorities, sector regulators, and SAIs. Developing formal inter-institutional cooperation protocols, as demonstrated by India's CAG-UIDAI coordination model, significantly strengthens SAI oversight effectiveness without requiring commensurate increases in audit staffing.

**Incremental deployment with audit gates:** Rwanda's experience demonstrates that phasing DPI deployment with mandatory IS audit review points at each stage provides SAIs with structured access and a manageable audit scope, a practical model for resource-constrained SAIs. ASSL can advocate for this approach within Sierra Leone's forthcoming National Digital Transformation Strategy, ensuring that IS audit readiness keeps pace with DPI expansion.

## 6. A DPI Audit Maturity Model for Low- and Middle-Income Countries

Drawing on the foregoing analysis, this article proposes a DPI Audit Maturity Model (DPI-AMM) for LMICs, structured around four audit dimensions and five maturity levels: Initial, Developing, Defined, Managed, and Optimizing. The four dimensions are:

1. **Digital Identity Integrity**: authentication security, coverage equity, and legal framework compliance.
2. **Payment System Reliability:** uptime assurance, transaction integrity, and interoperability standards.
3. **Data Governance:** privacy protection, consent mechanisms, and breach response.

4. **Equity Performance:** demographic penetration rates, accessibility compliance, and exclusion remediation. Table 1 presents the full indicator matrix.

***Table 1: DPI Audit Maturity Model (DPI-AMM) — Dimensions and Key Indicators***

| Audit Dimension | Initial | Developing | Defined | Managed / Optimizing |
|---|---|---|---|---|
| **Digital Identity Integrity** | No IS audit of identity systems | Ad hoc IS reviews conducted | Formalized IS audit methodology | Continuous monitoring; equity metrics embedded |
| **Payment System Reliability** | No audit capacity | Basic transaction reviews only | Interoperability standards audited | Real-time audit analytics deployed |
| **Data Governance** | No data protection audit | Compliance checks initiated | Privacy framework fully audited | Algorithmic accountability assessed |
| **Equity Performance** | No equity metrics used | Limited demographic analysis | Equity KPIs in audit plan | Exclusion remediation tracked & reported |

*Source: Author's compilation based on ISSAI 5300, COBIT 2019, and CDPI (2023)*

ASSL's current position across these dimensions is assessed as predominantly Initial to Developing, reflecting the absence of formalized IS audit methodologies, limited certified technical staffing, and nascent DPI infrastructure. Figure 3 visualizes ASSL's current positioning relative to the AFROSAI-E average and a proposed three-year target trajectory. The international benchmarks in Section 5 inform this roadmap: rights-by-design audit standards (EU eIDAS model) anchor the Defined level, while federated oversight coordination (India CAG model) and audit-gated deployment (Rwanda model) characterize the Managed and Optimizing levels respectively.




**Figure 3:** ASSL DPI-AMM Positioning — Current, AFROSAI-E Average, and 3-Year Target

*Source: Author's own compilation based on AFROSAI-E Survey (2022) and DPI-AMM framework*

## 7. Discussion and Conclusion

Digital Public Infrastructure (DPI) holds transformative potential for inclusive governance in Sierra Leone and across Sub-Saharan Africa by extending public-service reach, reducing transaction costs, and strengthening accountability through shared digital foundations for identity, payments, and data exchange. However, the evidence from Figures 2 and 3 and Table 2, together with international experience from India, the EU, Rwanda, and Ghana, demonstrates that these benefits depend on robust and independent IS audit oversight. For ASSL, strengthening audit capacity requires formalised methodologies, targeted technical capacity development, and inter-institutional coordination. The DPI Audit Maturity Model (DPI-AMM) provides a practical pathway towards the Defined level, focusing on digital identity integrity, payment-system reliability, data governance, and equity performance.

Accordingly, ASSL should develop a dedicated DPI Audit Framework aligned with ISSAI 5300 and COBIT 2019; the Government of Sierra Leone should incorporate explicit audit and accountability provisions into the forthcoming National Digital Transformation Strategy; AFROSAI-E should develop a regional DPI Audit Toolkit incorporating rights-by-design criteria; and INTOSAI's WGITA should issue supplementary guidance on DPI auditing. DPI is not merely a technological phenomenon; it is a governance choice. Building DPI as an open, equitable, and accountable

public good requires deliberate institutional architecture and robust SAI oversight. SAIs that position themselves at the forefront of DPI accountability can fulfil their constitutional mandates while contributing to inclusive and transparent governance in the digital age.

## References

AFROSAI-E. (2022). IT audit framework for African supreme audit institutions. African Organization of English-speaking Supreme Audit Institutions.

Audit Service Sierra Leone. (2023). Annual report 2022. ASSL.

Centre for Digital Public Infrastructure. (2023). DPI and governance: A framework for inclusive digital transformation. CDPI. https://cdpi.dev

European Commission. (2024). The European digital identity framework: eIDAS 2.0. European Commission. https://digital-strategy.ec.europa.eu

G20 Digital Economy Working Group. (2023). G20 New Delhi Declaration on digital public infrastructure. G20 Secretariat.

International Organization of Supreme Audit Institutions. (2016). ISSAI 5300: Guidelines for IT audit. INTOSAI. https://www.issai.org

ISACA. (2018). COBIT 2019 framework: Governance and management objectives. ISACA.

United Nations. (2020). Roadmap for digital cooperation: Report of the Secretary-General (A/74/821). United Nations. https://www.un.org/en/content/digital-cooperation-roadmap

World Bank. (2022). Identification for development (ID4D): Annual report 2022. World Bank Group. https://id4d.worldbank.org

World Bank. (2023). Digital government readiness assessment: Sierra Leone. World Bank Group. https://www.worldbank.org

# The Technological Crossroads: Challenges and Opportunities of Digital Public Infrastructure in Cuba


## Makisleidis Esponda Bravo

Ministry of Foreign Trade and Investment, Cuba





## Abstract

The digital transformation of the public sector in Cuba is undergoing a crucial phase marked by the implementation of the Cuban Digital Agenda 2030. This article analyzes the current state and challenges of the Digital Public Infrastructure (DPI) in the country. Using a qualitative and descriptive approach based on the documentary analysis of government regulations, sector reports, and recent specialized literature, the main local payment and digital identity platforms are evaluated. Key findings demonstrate that, while the initial stages of presence and interaction through institutional citizen service portals and digital payment platforms (such as Transfermóvil and Enzona ) have been consolidated, the complete transaction phase faces severe structural limitations. Among the main obstacles are the technological obsolescence of the network infrastructure, the persistence of territorial digital divides, the lack of an interoperable culture among public administration agencies, and the scarcity of financial resources for sustained investment. In conclusion, the article argues that the success of digital literacy in Cuba depends not only on the adoption of computer tools, but also on the development of a comprehensive regulatory framework, the strengthening of citizens' digital literacy, and the optimization of internal state processes to guarantee true social inclusion and technological sovereignty under the current complex economic conditions.



## Keywords

Digital Public Infrastructure, Digital Government, Financial Inclusion, Cuba, Interoperability, Technological Sovereignty.

## 1. Introduction

The concept of Digital Public Infrastructure (DPI) refers to the set of shared systems (such as digital identity, payment gateways, and secure data exchange) that enable the efficient delivery of public and private services across society. In Cuba, this process is not merely a technical modernization; it is positioned as a national security priority within the "Comprehensive Policy for Improving the Informatization of Society" (Ministry of Communications [Mincom], 2019). With the approval of the Policy for Digital Transformation, the Cuban Digital Agenda, and the Artificial Intelligence Strategy, the country seeks to develop a technological ecosystem that supports digital government, financial inclusion, and the simplification of procedures, operating under a unified model coordinated from the highest executive level.

The digitization process in Cuba has developed at a unique pace. Following the widespread adoption of mobile internet access since late 2018 and the gradual expansion of telecommunications infrastructure, the island experienced a forced acceleration in the adoption of digital services during the health crisis caused by the COVID-19 pandemic.

The purpose of this article is to diagnose the current state of Cuban digital billing (DBI) development at its current stage of maturation. To this end, the objectives focus on identifying the strengths of local payment channels, analyzing the barriers to integrating civil data, and reflecting on the gap between government guidelines and the actual user experience. Understanding these dynamics is crucial because Cuba is implementing its digitization under conditions of an external financial blockade imposed by the United States, which necessitates seeking viable local alternatives and open-source models for its administration.



## 2. Main Content

Fundamental Pillars of IPD in Cuba: Channel Analysis and Adoption

The deployment of the IPD in Cuba rests on three fundamental pillars that seek the automation of public life and administrative simplification: centralized citizen identification, sovereign payment gateways, and integration of government portals.

### A- Digital Identity

**Sovereignty Platform (www.soberania.gob.cu):** Launched with the central focus of digital citizen identity in the country. It allows for the secure authentication of individuals to interact with the public administration.

**Electronic Signature:** Implemented across the board for natural and legal persons, providing legal validity to digital acts and documents, and reducing mandatory in-person attendance at public registries.

Essential for transitioning from informational to transactional governance is the **Single Citizen Registry**, managed jointly by the Ministry of the Interior (Minint), the Ministry of Justice (Minjus), and technology entities. This unified registry has enabled the implementation of platforms for online requests for official notarial certificates (birth, marriage, criminal records) validated using a Secure Verification Code (CSV) and electronic signature. The integration of the **Soberanía** government procedures platform with the EnZona identity provider illustrates the efforts to centralize citizen credentials.

### B- Payment Gateway and Financial Inclusion.

Within the framework of the banking process and the minimization of the use of cash, the financial IPD is based on two sovereign platforms that act as public payment channels:

**Transfermóvil** : Developed by the Telecommunications Company of Cuba SA(ETECSA) , consolidated as the gateway with the greatest reach for payment of services (electricity, water, telephone, taxes) and the retail e-commerce ecosystem.

**Table No. 1: Statistics showing the use of Transfermovil in the country .**

| Operational Indicator | Metric/Current Status | Social Impact |
|---|---|---|
| Transaction volume | It exceeds 1 billion transactions annually. | It sustains the daily flow of domestic transfers in the absence of cash. |
| Growth rate | Stable year-on-year increase of 18%. | It demonstrates widespread and mandatory adoption in formal trade. |
| User acquisition | Addition of more than 1,100 new users daily. | Constant expansion of the digitally banked customer base. |
| Service integration | Payment for electricity, water, gas, telephone and taxes | Drastic reduction in transaction costs and in-person waiting times. |

**EnZona:** Developed by the Information Technology Company for Defense(Xetid) focused primarily on e-commerce, payment gateways for virtual stores and the management of transactions for both state and non-state management forms(MSMEs and cooperatives).

**Table No. 2: Differences and structural comparison of these payment ecosystems.**

| Platform | Developer | Technological Approach | Strengths | Key Limitations |
|---|---|---|---|---|
| Transfermovil | ETECSA | Secure text messaging (USSD and Internet codes) | Highly inclusive, it works without active mobile data. | Less visual and more rigid user interface |
| InZone | XETID | Web and mobile platform based on QR code and the Internet | Greater ease of use for physical and electronic businesses. | It depends strictly on an active data connection |

## C- Interoperability and Data Exchange.

**Digital Government Ecosystem:** The central challenge of the current regulatory framework is the interconnection of the databases of the Organs and Agencies of the Central State Administration (OACE).

The "Citizen Portals" which cover all provinces of the country, were originally designed to bring transparency to the local management of municipal governments. However, empirical reviews indicate a pattern of "static reading sites" (del Campo, 2024). Mechanisms for direct interaction or the resolution of legal procedures entirely remotely are limited due to the lack of robust servers integrated with national legal databases.

The simplification and integration of procedures is prioritized to prevent citizens from having to hand over documents that are already in the possession of the State (such as birth certificates or background checks), moving towards open and interoperable data systems under strict cybersecurity standards.

### Telecommunications Infrastructure and Technical Support

For the logical and software layers to function, Cuba continues to expand its physical and connectivity infrastructure, managed by the national operator ETECSA:

a) **Access and Mobile Network:** Prioritizing the intensive expansion of the 4G network and the gradual introduction of infrastructure capabilities ready for the 5G standard, in addition to strengthening Voice over LTE (VoLTE) technology.

b) **International Connectivity:** Increased capacity of the country's Internet access points (the submarine cables with ALBA-1 and the Arimao system) to improve latency and resilience of the National Data Network.

c) **Edge and Cloud Computing**: Modernizing National Data Centers to offer cloud services to companies and public entities with differentiated rates, encouraging migration towards the Industry 4.0 model.

### IPD Governance in Cuba

The Governance of the Cuban Digital Environment has adopted a multi-sectoral character with a higher hierarchical level to avoid fragmented efforts:

- **Executive Leadership:** The Government Program for Digital Transformation is chaired directly by the Deputy Prime Minister and coordinated by the Ministry of Communications (MINCOM).
- **Strategic Pillars:** The agenda articulates its actions in key areas that include technological infrastructure, digital government, cybersecurity, the digital economy and innovation.
- **The Innovation Ecosystem:** Universities play a role as providers of scientific infrastructure, highlighting the Science and Technology Parks (such as those in the province of Havana and Matanzas) where academia, state-owned enterprises and new MSMEs in the software sector come together to develop the country's digital public goods.

### Critical Findings and Inclusion Gaps

Despite the high levels of quantitative adoption of payment gateways, the qualitative analysis of IPD in Cuba reveals contradictions and systemic barriers that condition its role as an enabler of inclusive governance.

- **Operational limitations of the banking system:** Although the IPD allows for agile transactions, the underlying financial ecosystem imposes strict limits on the number and amount of monthly transfers due to tax risk control. This creates a gap between the platform's technical capacity and the business needs of new economic actors (such as SMEs) and ordinary citizens.
- **Material digital divide and obsolescence:** Infrastructure requires devices with compatible operating systems. Lack of access to modern hardware due to low purchasing power and inflation restricts the participation of the most vulnerable sectors or the elderly, accentuating a generational adoption gap.
- **Centralization and concerns about data governance** : The deployment of electronic signatures and digital identities closely controlled by state-owned corporations linked to national defense sectors raises regulatory debates about data privacy. The absence of a transparent legal framework for personal data protection comparable to international standards limits the level of full public trust in the institutional environment.

## 3. Conclusions

The current landscape in Cuba reveals an accelerated, yet markedly asymmetrical, process of financial inclusion. While there is enthusiastic adoption of technological tools for everyday payments, accumulated deficiencies in the physical banking infrastructure continue to limit the true reach of the digital economy, especially for the elderly and residents of rural areas far from provincial capitals. This technological gap is exacerbated by a systemic incompatibility within the public administration: the development of local platforms based on open-source software clashes head-on with a rigid bureaucratic culture, unaccustomed to the horizontal exchange of information between different ministries.

This reality presents a crucial dilemma between sovereignty and resilience. Although the design of native cybersecurity and data governance solutions (Reyes, 2026) is a key defense for national sovereignty, the low availability of state-of-the-art telecommunications hardware infrastructure severely limits the system's ability to respond to recurring contingencies, such as blackouts or network traffic spikes.

To advance toward this model of inclusive governance, it is essential to structure three indispensable lines of action. First, interoperability and technological neutrality must be guaranteed, fostering open standards that allow independent developers and non-state management entities to integrate equitably into public data networks without falling into corporate or state monopolies. Second, it is vital to design effective inclusion policies that offer simplified e-government interfaces with free navigation for the user (zero-rating), while also ensuring that efficient physical service channels are maintained so as not to leave behind the population that lacks smartphones or digital literacy. Finally, it is urgent to strengthen the legal framework for privacy through public and independent audits of sensitive systems such as the

Single Citizen Registry, so that the centralization of personal data does not, under any circumstances, degenerate into tools of exclusion or surveillance.

In conclusion, Cuba possesses a highly valuable human capital and a proven capacity to develop creative and robust solutions in the face of extreme economic scarcity. However, the ultimate success of the island's Digital Public Infrastructure will not be achieved by simply adding isolated web portals or disconnected procedures; it will depend entirely on the will to consolidate a unified, horizontal digital ecosystem truly centered on the everyday needs and rights of citizens.

## References


Citations in the text:

...of the Improvement of the Informatization of Society in Cuba (Ministry of Communications [Mincom], 2019).

...preserves the country's sovereignty and optimizes security resources (Reyes, 2026).

Bermúdez, MDC (2021). Innovation-oriented government management: Context and characterization of the model. Cubadebate . http://www.cubadebate.cu/especiales/2021/03/01/gestion-del-gobierno-orientado-a-la-innovacion-contexto-y-caracterizacion-del-modelo/

del Campo, MG (2024). Digital government in Cuba: analysis of the digital ecosystem related to online services. Cuban Journal of Digital Transformation, 5(1), 45–62.

Ministry of Communications. (2019). Comprehensive Policy for the Improvement of the Informatization of Society in Cuba. Mincom .

Reyes, AB (2026). Autonomic solution for the comprehensive management of cybersecurity based on reinforcement learning. Tono, Technical Journal of the Telecommunications Company of Cuba SA, 21(1), 12–23.



Section VII

# THE NEXT HORIZON: AI, DIGITAL TWINS AND ANTICIPATORY ASSURANCE

# Auditing Digital Public Infrastructure in the Age of Artificial Intelligence: A Vietnamese Perspective on Moving toward Proactive Public Audit

**Tran Thi My Giang**
State Audit Office of Vietnam



## Abstract

Digital Public Infrastructure (DPI) is changing the environment in which governments deliver services, manage public resources and communicate with citizens. For Supreme Audit Institutions (SAIs), this development raises a practical question: how can public audit remain relevant when financial and administrative data are created continuously through digital systems? This article discusses the role of artificial intelligence (AI) and data analytics in supporting the audit of DPI, with reference to recent developments in the State Audit Office of Vietnam. It considers how AI can assist auditors in audit planning, risk identification, public procurement analysis, review of digitized records and quality control of audit reports. The article does not treat technology as a replacement for audit judgment. Instead, it views AI as a tool that can help auditors work with larger datasets and identify risk signals earlier. Its value depends on reliable data, cybersecurity, legal clarity, sound audit methodology and professional skepticism. The Vietnam experience suggests that AI can support a gradual movement from mainly post-audit work toward a more proactive and data-informed model of public audit, while human responsibility remains central.

## Keywords

Digital Public Infrastructure; Public Audit; Artificial Intelligence; Data Analytics; Accountability; Inclusive Governance.

## 1. Introduction

Digital transformation has changed the daily working environment of public administration. In Vietnam, as in many other countries, public services and public financial management are increasingly supported by information systems, electronic records and online platforms. Procurement, budget management, tax administration, social insurance, public investment and service delivery now generate a large amount of data every day.

This creates real opportunities for governance. Digital systems can reduce manual procedures, make transactions easier to trace and help public agencies respond more quickly. At the same time, they also raise new questions for auditors. If data are incomplete or inconsistent, the conclusions drawn from them may be weak. If systems are not secure, sensitive information may be exposed. If online services are difficult for some groups to access, digital transformation may unintentionally create exclusion rather than inclusion.

For Supreme Audit Institutions, these are not merely technical matters. They affect how auditors plan their work, collect evidence, assess risks and report findings. Manual review and sample-based testing remain necessary, but they may not be enough when auditors deal with large and continuously updated datasets. A sample can still provide useful evidence, but it may not reveal wider patterns hidden in a much larger population of transactions.

AI and data analytics can help auditors respond to this environment. They can support the screening of large datasets, the identification of unusual patterns, comparison of records across entities and review of draft reports. Still, AI should not be seen as a shortcut to audit conclusions. It is better understood as a tool that helps auditors ask sharper questions and focus their professional judgment where risk appears higher.

This article discusses the use of AI and data analytics in auditing Digital Public Infrastructure, drawing on recent developments in the State Audit Office of Vietnam and on wider discussions on AI in public sector audit.

## 2. Digital Public Infrastructure and the Audit Challenge

Digital Public Infrastructure refers to foundational digital systems that support public services and public governance at scale. It may include digital identity, payment systems, data exchange platforms, public registries, service portals and related standards. In practice, DPI is not only about software or hardware. It is also about how data are governed, how institutions coordinate, how citizens access services and how public trust is protected.

A well-functioning DPI can contribute to inclusive governance. Citizens may access services more conveniently. Public agencies may exchange information more efficiently. Policymakers may rely on better data for decisions. Businesses and individuals may also interact with government in a more transparent and predictable way.

However, DPI can also concentrate risks. If one digital system has weak controls, the resulting risks may have wider impacts. If data-sharing arrangements are unclear, privacy and accountability may be affected. If a system records transactions but the data are incomplete or difficult to compare, auditors may have limited confidence in using that information.

For SAIs, auditing DPI therefore requires attention to both performance and controls. Auditors may need to ask whether digital systems are reliable, whether access controls are adequate, whether transactions are complete and traceable, whether public services reach intended users and whether digital platforms improve public outcomes rather than simply changing administrative procedures.

These questions show why the audit of DPI cannot rely only on traditional document review. It requires the ability to understand systems, follow data flows and analyze large volumes of information. INTOSAI guidance on information systems audit also reflects this need to consider systems, controls and audit evidence in a structured manner (INTOSAI, 2019).

## 3. From Post-Auditing to a More Proactive Audit Approach

In a traditional audit model, many procedures are performed after the audited period has ended. Auditors examine documents, select samples, verify compliance and issue findings. This remains an important part of public audit. However, in a digital environment, waiting until after transactions have occurred may reduce the possibility of early warning.

Recent discussions in Vietnam have emphasized the need to move from “post-auditing” toward “smart, proactive and real-time auditing” (Vietnam News Agency, 2025). This should not be understood as a replacement for established audit principles. Rather, it reflects a practical need to use available digital data more effectively so that auditors can identify risks earlier and allocate audit resources more appropriately.

The State Audit Office of Vietnam has been developing digital transformation as one of the important directions for audit modernization. AI and data-driven applications have been explored in areas such as budget data analysis, risk assessment, financial transaction review, public investment monitoring and audit quality control. These applications are closely linked to DPI because they depend on the availability, quality and governance of public digital data.

The change is not simply about using a new tool. It also changes the rhythm of audit work. Instead of spending most of the time searching manually through records, auditors can use analytical tools to locate unusual patterns, compare data and identify areas that deserve closer review. The auditor’s role then becomes more focused on verification, explanation and professional assessment.

**Figure 1. From traditional post-auditing to proactive digital audit**

| Traditional post-auditing | Proactive digital audit supported by AI and data analytics |
|---|---|
| Audit work is mainly performed after transactions have occurred | Audit work can be supported by earlier risk signals from digital data |
| Audit procedures rely heavily on sample-based testing | Audit procedures may include wider data screening and population analysis |
| Auditors manually review documents and records | Auditors use analytics to compare, filter and prioritize records |
| Findings are often corrective in nature | Recommendations may become more preventive and timely |
| Systemic risks may be difficult to detect from small samples | Broader analysis may help reveal patterns across entities or periods |
| Audit evidence is mainly collected through selected files | Audit evidence can be supported by digital records and cross-data comparisons |

*Source: Author's illustration based on recent discussions on the transition from post-auditing to smart and proactive auditing.*

## 4. AI Applications in the Audit Cycle

The use of AI in auditing can be considered across different stages of the audit cycle. In planning, AI can support the selection of audited entities. By using available data and risk indicators, auditors can compare entities, sectors or programmes before deciding where to focus audit resources. This is useful because SAIs often work with limited time and staff while the scope of public sector activities continues to expand.

During audit implementation phase, data analytics can help auditors examine large datasets. In public procurement, for instance, analytical tools may help identify repeated suppliers, unusual bidding patterns, short implementation periods, abnormal contract values or other indicators that require further review. In social insurance, tax administration or budget management, data analysis may help detect inconsistencies, duplicate records or unusual trends.

Vietnam's experience also shows the usefulness of AI in reviewing digitized records. Automated tools can support the collection and initial screening of documents from digital platforms. This allows auditors to compare information across localities or units instead of reviewing each file separately and manually. In some cases, such comparisons may reveal differences that would be difficult to see through traditional audit work.

AI can also support audit quality control. One possible application is to compile audit reports from previous years and create a knowledge base for auditors and reviewers. Such a system may

help compare similar findings, improve consistency of recommendations and identify missing or inconsistent information in draft reports. This is especially useful in a large audit institution where similar audit issues may arise in different localities or audit units.

Still, AI should be used with caution. An AI-generated signal is not an audit finding. A risk score is not audit evidence by itself. Auditors must verify the information, understand the context, assess materiality and decide whether sufficient and appropriate evidence exists. This is consistent with the view that AI can assist auditors but cannot replace their intuition and professional experience (CafeF, 2025).

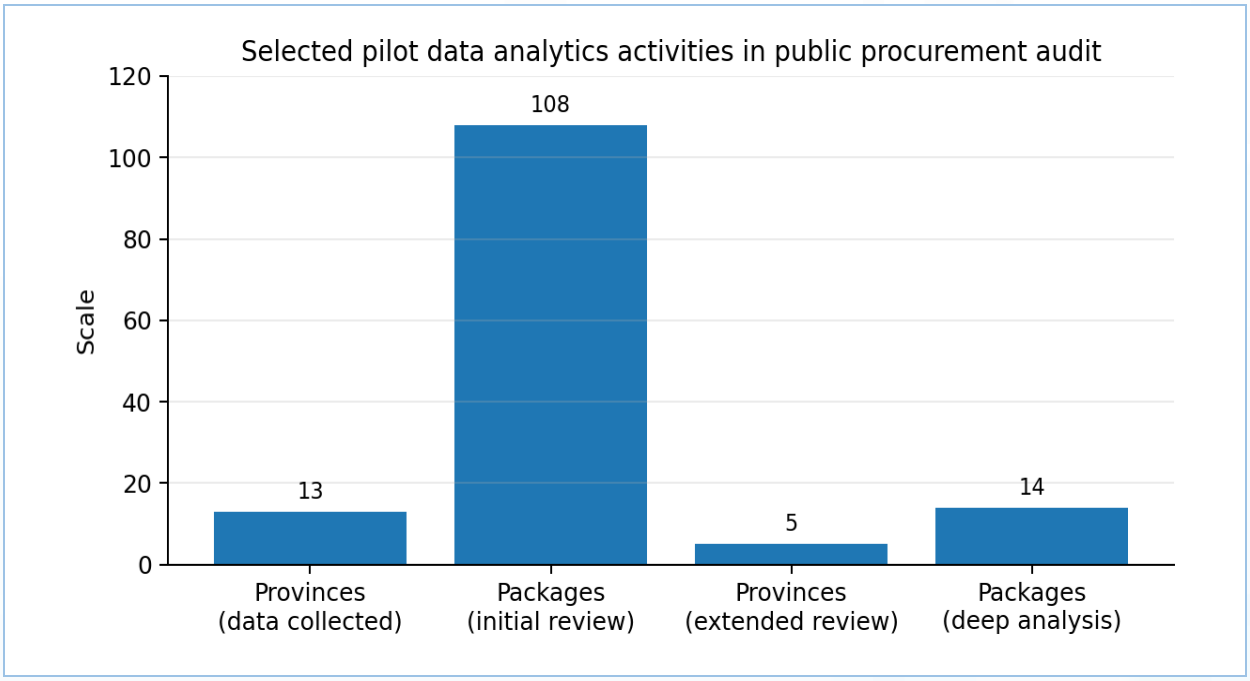
**Table 1. Selected AI-enabled applications in the public audit cycle**

| Audit stage | Possible AI-enabled application | Expected contribution to public audit |
|---|---|---|
| Audit planning | Risk-based selection of audited entities | Supports prioritization of higher-risk entities, sectors and programmes |
| Data collection | Automated collection of digital records from public platforms | Reduces manual work and expands preliminary review |
| Audit implementation | Analysis of procurement, budget, financial and administrative datasets | Helps identify unusual patterns, inconsistencies and potential risks |
| Evidence review | Comparison of data across entities, localities and periods | Supports detection of issues that may not be visible from isolated manual review |
| Audit reporting | AI-assisted review of draft audit reports | Improves consistency, completeness and quality control |
| Follow-up and learning | Knowledge base from previous audit reports and recommendations | Supports retrieval of audit experience and consistency of recommendations |

*Source: Compiled by the author based on recent developments in the State Audit Office of Vietnam.*

A practical example can be seen in pilot data analytics activities in public procurement audit. Reported activities included data collection from 13 provinces, initial analysis of 108 procurement packages, extended review in 5 provinces and deeper analysis of 14 packages (N. Loc & N. Hong, 2025). These figures are modest compared with the total volume of public procurement activity, but they show a useful direction: digital tools can help auditors screen a wider population before conducting detailed verification.

**Chart 1. Selected pilot data analytics activities in public procurement audit**




*Source: Compiled by the author from reported pilot activities of the State Audit Office of Vietnam.*

## 5. Contribution to Inclusive Governance

The connection between AI-enabled auditing and inclusive governance lies in accountability. DPI can help governments serve citizens better, but this benefit can only be sustained if digital systems are reliable, secure and properly managed.

AI-supported audit can contribute to inclusive governance in practical ways. Wider data analysis can reduce the risk that important issues are missed because they fall outside a small audit sample. Earlier risk detection can help public agencies correct weaknesses before they become larger problems. Stronger data-based evidence can make audit findings more persuasive and recommendations more useful.

The audit of DPI can also help ensure that digital transformation benefits citizens in practice. Auditors can assess whether systems are accessible, whether data are protected, whether transactions are traceable and whether public services reach intended beneficiaries. These are important questions because inclusive governance is not achieved simply by creating digital platforms. It requires that those platforms serve the public fairly and effectively.

In this sense, AI-enabled auditing supports more than audit efficiency. It can help strengthen public trust by showing that digital government systems are subject to independent review and that public resources remain accountable in the digital environment.

## 6. Safeguards and Risks

AI brings opportunities, but it also brings risks that SAIs must manage carefully. The first issue is data quality. AI and analytics depend on reliable data. If data are incomplete, inconsistent or scattered across different systems, analytical results may be misleading. Data standardization, interoperability and clear data-sharing arrangements are therefore necessary foundations for digital auditing.

The second issue is cybersecurity and confidentiality. Public sector auditing often involves sensitive financial, administrative and personal information. If AI tools are used without proper safeguards, confidential information may be exposed. SAIs need secure infrastructure, access control and clear procedures for handling data.

The third issue is overreliance on technology. AI outputs may appear objective, but they are influenced by the data, assumptions and models used. Auditors should not accept AI-generated results without verification. Professional skepticism remains essential. A suggested anomaly should be treated as a starting point for further audit procedures, not as a final conclusion.

Generative AI requires particular caution. Large language models can support summarization, translation, drafting and document review. However, they may also produce inaccurate information or create false references. They may also create confidentiality risks if sensitive information is entered into publicly available tools. The Canadian Audit and Accountability Foundation has similarly highlighted risks relating to inaccurate AI outputs, overreliance and confidentiality when publicly available AI tools are used in audit work (Canadian Audit and Accountability Foundation, 2024).

Finally, auditor capacity is a key condition. Auditors need to understand not only how to operate digital tools, but also how to interpret results and document evidence. A modern public auditor does not need to become a data scientist, but should be able to ask informed questions about data, systems and analytical outputs.

## 7. Human Judgment Remains Essential

A consistent lesson from Vietnam's discussion on AI in auditing is that AI cannot replace the intuition, experience and professional judgment of auditors. Public audit is not only a technical exercise. It involves legal responsibility, institutional understanding and the public interest.

AI may detect an unusual pattern, but it cannot fully explain why that pattern occurred. It may compare documents, but it cannot determine by itself whether an audit recommendation is fair, feasible and legally sound. It may help review a report, but it cannot take responsibility for the audit conclusion.

This point is important for public trust. The credibility of an SAI depends on independence, integrity, evidence and professional responsibility. Technology can strengthen audit work when used properly, but it can also weaken audit quality if auditors rely on it mechanically.

The better approach is not to choose between auditors and machines, but to combine them. AI can help auditors see more, compare faster and identify risks earlier. Auditors remain responsible for deciding what those signals mean and whether they are supported by sufficient evidence.

## 8. Practical Lessons for SAIs

Several practical lessons may be drawn from the Vietnamese experience. The first is that AI should begin with real audit needs. It should not be adopted only because it is new. It should help answer audit questions, improve risk assessment, widen audit coverage or strengthen report quality.

The second lesson is that data governance should come before advanced analytics. Without reliable and accessible data, AI applications will have limited value. SAIs need to work with public agencies to improve data access and data standards, while maintaining audit independence.

The third lesson is the importance of pilot projects. Pilots allow audit institutions to learn gradually. Through them, auditors can identify data limitations, test analytical methods and build internal capacity before expanding implementation.

The fourth lesson is that audit methodology needs to evolve. AI-supported outputs must be linked to audit evidence, documentation standards and quality control procedures. Auditors need guidance on how to explain and use digital analysis in audit files and reports.

Finally, ethical and security safeguards should be built into AI use from the beginning. Confidentiality, privacy, cybersecurity and accountability should not be treated as later concerns.

## 9. Conclusion

Digital Public Infrastructure is reshaping the environment of public governance. For SAIs, it creates both a challenge and an opportunity. The challenge is that traditional audit methods may not fully address large, complex and continuously updated digital systems. The opportunity is that AI and data analytics can help auditors examine public data more effectively, detect risks earlier and strengthen evidence-based accountability.

The experience of the State Audit Office of Vietnam shows that AI can support a shift from post-auditing toward more proactive and data-informed auditing. Practical applications in audit planning, procurement analysis, digitized record review and audit quality control demonstrate the potential of technology to improve audit efficiency and audit coverage.

However, AI must be used responsibly. Data quality, cybersecurity, legal clarity, auditor capacity and professional judgment are essential. AI should support auditors, not replace them. In auditing DPI, human responsibility remains central because audit findings affect public institutions, public resources and citizens' trust.

When used carefully, AI-enabled auditing can help SAIs strengthen public accountability in the digital era. It can also help ensure that DPI serves not only administrative efficiency, but also inclusive governance and the public interest.

## References

CafeF. (2025, August 21). Deputy Auditor General: AI can analyze finances and input data, but the intuition and experience of auditors are something that AI cannot replace.

Canadian Audit and Accountability Foundation. (2024). Can ChatGPT write your next audit? Using generative AI to power your audit. CAAF Webinar Program.

Do Huu. (2025, May 26). Applying AI, a new technology – the "key" to creating breakthroughs in auditing activities. Audit Newspaper.

INTOSAI. (2019). GUID 5100: Guidance on audit of information systems. International Organization of Supreme Audit Institutions. https://www.issai.org/pronouncements/guidance-on-audit-of-information-systems/

N. Loc & N. Hong. (2025, July 24). State Audit Office: Ready to apply AI. Audit Newspaper.

OECD. (2019). OECD AI Principles. Organisation for Economic Co-operation and Development. https://www.oecd.org/en/topics/sub-issues/ai-principles.html

UNDP. (n.d.). Digital Public Infrastructure (DPI). United Nations Development Programme. https://www.undp.org/digital/digital-public-infrastructure

Vietnam News Agency. (2025, October 13). AI is helping to shift from "post-auditing" to "smart, proactive auditing".

VnExpress. (2025, August 21). Sẽ dùng AI kiểm soát chất lượng báo cáo kiểm toán.

World Bank. (2025). Digital Public Infrastructure and Development: A World Bank Group Approach. World Bank Group.

# Building Tomorrow, Today: How Digital Twins are reshaping India's Infrastructure journey to 2047

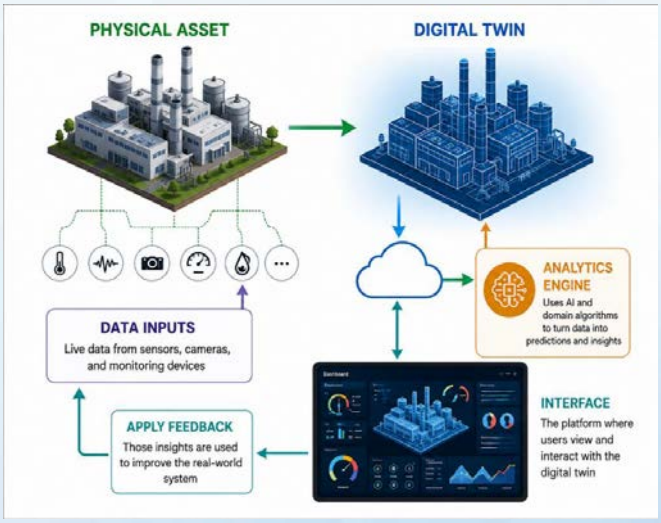
**Piyush Tiwari**
O/o the Comptroller & Auditor General of India



## Abstract

India is entering a decisive phase in its infrastructure journey as it moves towards the Amrit Kaal vision of India@2047 and an economy of USD 35–40 trillion. Achieving this ambition will require sustained investment in highways, railways, airports, urban infrastructure, ports and other critical assets, along with stronger mechanisms to ensure that public expenditure delivers value. Initiatives such as PM Gati Shakti, Sagarmala and the National Investment and Infrastructure Fund (NIIF) have strengthened integrated infrastructure development; however, project delays, cost overruns, fragmented planning and increasing climate risks continue to pose significant challenges.

Against this backdrop, Digital Twin technology offers an opportunity to transform not only how infrastructure is planned and managed, but also how it is audited. A Digital Twin is more than a 3D model—it is a dynamic digital representation of a physical asset, system or process, continuously updated through data from Geographic Information System (GIS), Building Information Modelling (BIM), Internet of Things (IoT) sensors, Global positioning System (GPS), operational systems and other sources. When combined with Artificial Intelligence (AI), analytics and



simulation, it can provide a near-real-time view of an asset's condition and performance, enabling stakeholders to identify risks, test scenarios, predict failures and make better decisions across the infrastructure lifecycle.

This has particular relevance for the Office of the Director General of Audit (Infrastructure), Delhi, which audits major infrastructure sectors and entities such as National Highways Authority of India (NHAI), Delhi Development Authority (DDA), Central Public Works Department (CPWD), Airports Authority of India (AAI), Delhi Metro Rail Corporation (DMRC), National Buildings Construction Corporation (NBCC) (India) and other Central Public Sector Enterprises (CPSEs) under the Ministry of Housing and Urban Affairs, Ministry of Civil Aviation and Ministry of Road Transport and Highways.

Digital Twins could enable a shift from predominantly static, document-based audit evidence towards data-rich, continuously updated audit environments. Instead of examining an infrastructure asset only through files, physical inspections and historical records, auditors could potentially use its digital counterpart to analyse project progress, asset utilisation, maintenance patterns, contract performance and emerging risks through a consolidated view.

India has already begun exploring this potential through initiatives such as the AI-powered Digital Twin at Hyderabad Airport, the 3D urban spatial twin of Varanasi, Digital Twin applications explored for Indian Railways, and the Sangam: Digital Twin initiative of the Department of Telecommunications. These developments indicate that Digital Twins are gradually moving from a conceptual technology to practical applications in Indian infrastructure.

The article examines the evolution, applications and audit potential of Digital Twins, while also considering challenges such as data quality, interoperability, cybersecurity, high initial investment, standardisation and availability of skilled personnel. It proposes that Digital Twins can become an important component of the future infrastructure-audit ecosystem, helping auditors move from a predominantly historical and compliance-oriented approach towards more continuous, risk-based and data-driven assurance. For India@2047, the technology therefore represents not merely a smarter way of managing infrastructure, but a potential new paradigm for ensuring that the infrastructure being created today remains efficient, resilient, sustainable and accountable throughout its lifecycle.

## (i) India’s infrastructure in a shifting global landscape

India’s infrastructure vision is anchored in its ambitions for economic transformation and global competitiveness. At the core is Vision 2047, envisioning India as a USD 40 trillion economy by its centenary year—backed by sustained capital allocation to modernize critical infrastructure, including energy, transport, urban services, and digital systems.

Initiatives such as PM Gati Shakti, the Asset Monetisation Programme, and the National Investment and Infrastructure Fund (NIIF) continue to strengthen institutional capacity,

introduce structured investment pathways, and catalyse private-sector participation. These systemic developments signal a strategy calibrated for long-term, inclusive infrastructure growth. Further, India's infrastructure investments now represent a significant share of GDP.

India's infrastructure is becoming a core driver of its economic rise, not just a support system.

a. **Boosts productivity** – Better highways, freight corridors, and ports (like the Sagarmala Programme) cut costs and delivery times. A 10% gain in transport efficiency can raise GDP by 1–2%, and Indian exporters are becoming more competitive globally.

b. **Attracts investment** – Strong infrastructure pulls in capital. The National Investment and Infrastructure Fund (~$4.9B in assets) brings in global investors, and better roads/rail are linked to higher foreign investment in manufacturing and logistics.

c. **Smarter planning = better results** – PM GatiShakti connects highways, rail, and ports through unified planning, cutting delays and waste. This helped India jump from 54th to 38th in the World Bank's Logistics Performance Index.

d. **Eyes on 2047** – As India targets a $40 trillion economy, infrastructure will blend physical networks (roads, power, water) with smart tech (AI, IoT) and sustainability (green transport, net-zero goals) to stay globally competitive.

Infrastructure is no longer just about building roads and ports—it's about building India's economic edge on the world stage.

## (ii) Challenges on the Road to 2047

India has made real progress, but reaching Viksit Bharat 2047 will need big changes in how infrastructure is planned, funded, and built. Some key roadblocks remain:

a. **Delays and cost overruns** – Many projects run late and over budget, often due to land acquisition issues, contractor problems, and mid-project design changes. As of early 2024, over 38% of central sector infrastructure projects were delayed, with cost overruns crossing INR 4.6 trillion. This eats into returns and delays the benefits reaching people. Construction productivity also lags global standards, partly due to skill gaps and slow adoption of modern methods like modular construction and digital twins.

b. **Planning happens in silos** – Roads, ports, and urban transit are often built without talking to each other—industrial zones get roads but not synced port access; metros lack last-mile connections. PM GatiShakti is helping fix this, but true integrated planning across all government levels is still a work in progress. Without it, India risks wasted capacity and duplicated spending.

c. **Sustainability is still catching up** – As climate risks grow (extreme weather, rising sea levels, per IPCC projections), infrastructure needs to be climate-resilient and low-carbon. But green construction practices, renewable-powered operations, and circular economy

principles are still in early stages. Slow environmental clearances and a lack of standard green building codes make it harder to build sustainability into projects from the start.

To hit its 2047 goals, India needs to fix execution delays, break down planning silos, and fast-track sustainable, climate-ready infrastructure.

### (iii) From Challenges to Solutions

To hit its 2047 goals, India needs to act on three fronts: use better project management and digital tracking tools to reduce delays and cost overruns; make integrated planning a standard practice across sectors, not an exception; and enforce climate-resilient building standards while scaling up sustainable construction methods.

### (iv) Digital Transformation: A "Systems-of-Systems" Approach

India's infrastructure is entering a new phase—one where physical assets and digital technology work together as one connected system. Instead of managing roads, power, water, and communications separately, a "systems-of-systems" approach links them into a single, smart network.

The key technology driving this is the **Digital Twin**—a live, virtual replica of real infrastructure that constantly updates using data from sensors, GPS/mapping tools, and operational systems.



Combined with GIS mapping, predictive analytics, and smart design, Digital Twins let planners simulate different scenarios, improve performance, and catch maintenance issues before they turn into expensive problems. It's not just about managing individual assets either—it helps different government agencies coordinate in real time, turning planning into action more smoothly.

This connected, tech-driven approach helps India tackle urban growth and climate challenges head-on, while positioning the country as a global leader in smart, sustainable infrastructure.

## What Are Digital Twins?

**Definition:** A Digital Twin is a real-time virtual copy of a physical object, system, or environment. It uses data from IoT sensors, live analytics, and simulations to mirror how the real thing behaves—and even predict what might happen next.

**Why It Matters:** This technology serves as a significant game-changer for various industries by facilitating the development of more efficient, sustainable, and resilient systems. Through the integration of real-time data and advanced simulations, it empowers stakeholders to make smarter decisions that optimize performance and significantly reduce operational costs. Furthermore, the system is designed for long-term impact, enabling eco-friendly and resource-efficient designs by leveraging comprehensive scenario testing to ensure sustainability.

**Where It's Useful:** In terms of practical application, the technology is particularly useful within the field of architecture, where it enhances building design, improves energy efficiency, and facilitates intelligent smart building management. Additionally, it plays a crucial role in energy infrastructure by strengthening grid management and supporting the integration of renewable energy systems. Its capacity for predictive maintenance is also vital, allowing for the identification and resolution of potential issues before they escalate into failures.

Digital Twins let us test, monitor, and improve real-world systems virtually—before spending time and money doing it in the physical world.

Digital Twins are advancing fast and set to play a major role going forward—especially for asset-heavy organizations. They help bring together engineering, operations, and IT into one unified view, or even immersive experiences you can interact with.

This is made possible by combining a few key technologies: 3D visualization, reality modeling, mixed reality (AR/VR), and geotechnical engineering. Together, they create a complete picture of infrastructure—both what's underground and what's above ground.

This full-picture view leads to better decisions across the board—improving network reliability, keeping consumers and workers safer, staying compliant with regulations, and reducing environmental impact.

## Levels of digital twin integration

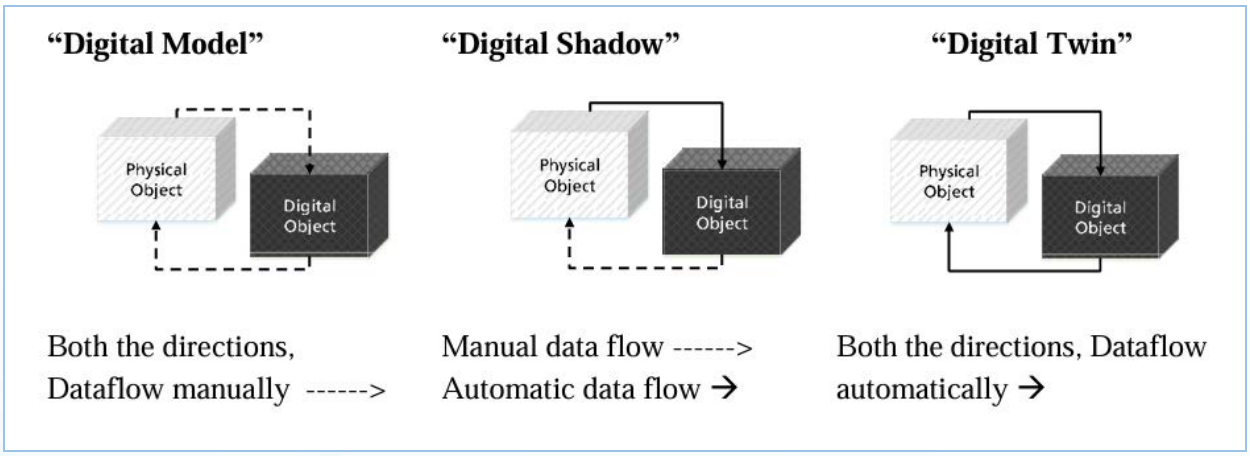
The terms "Digital Model," "Digital Shadow," and "Digital Twin" often get used interchangeably—but they actually represent different levels of connection between the physical and digital versions of something.

In manufacturing, a Digital Twin has been described as the point where physical and virtual products merge. In design and manufacturing, it's seen as a real-time digital copy of a physical object. What separates these three terms is how much automated data actually flows between the real object and its digital version:

- **Digital Model** – No automated data exchange at all. Any updates have to be made manually on both sides.
- **Digital Shadow** – One-way automated data flow. The physical object sends updates to the digital version, but not the other way around.

- **Digital Twin** – Two-way automated data flow. A change in either the physical or digital object automatically triggers a matching change in the other.

The key difference comes down to automation and direction of data flow—only a true Digital Twin has a live, two-way connection where both sides stay in sync automatically.



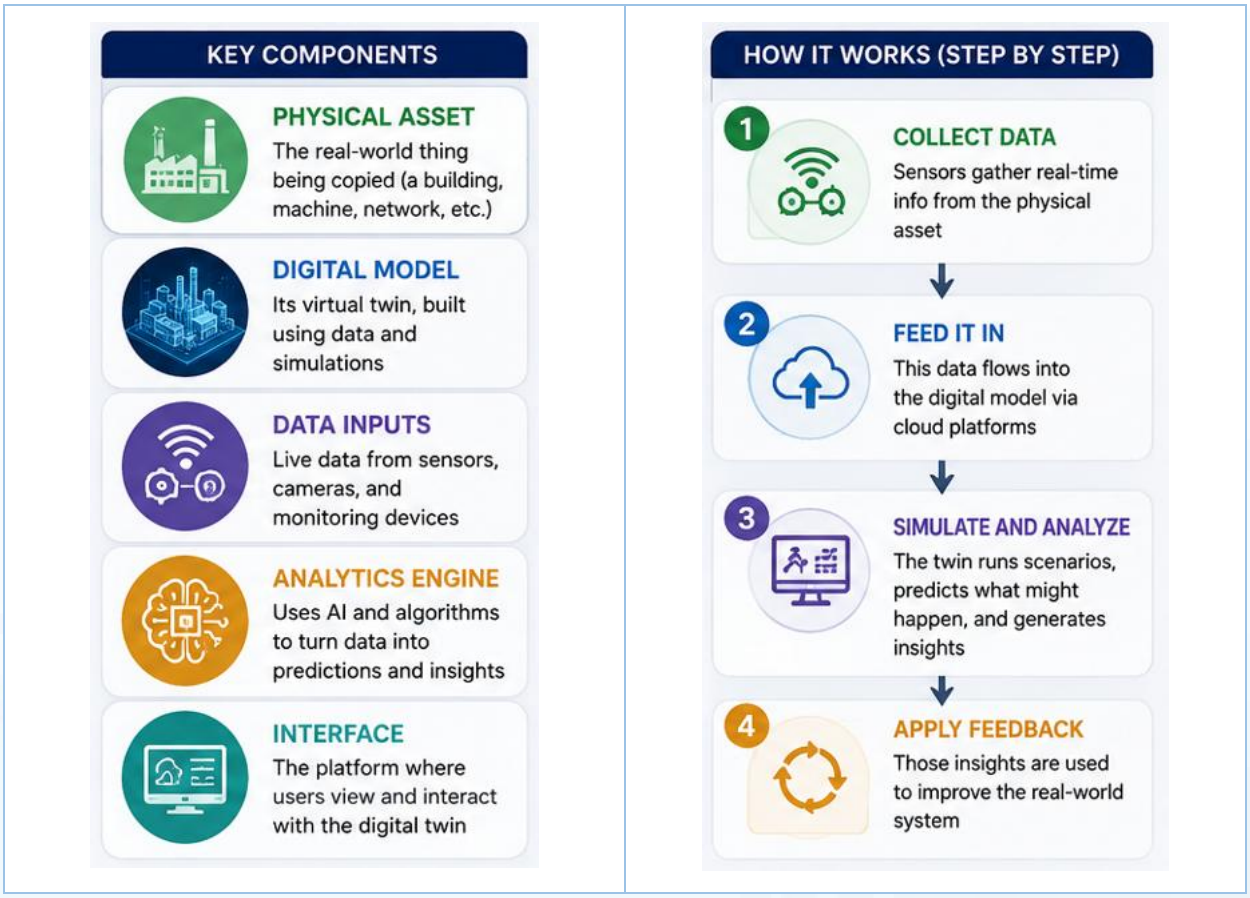

## Key Features of a Digital Twin

Digital Twins are changing how industrial facilities run by giving them a virtual copy of the physical plant that can be monitored, controlled, and improved. For a Digital Twin to actually work well, it needs these core features:

1. **Fidelity and Frequency** – Fidelity means how accurate and detailed the virtual model is—does it truly capture the asset's shape, behavior, and how it interacts with its surroundings? Frequency is about how often the data gets updated, which depends on the type of asset and how real-time the monitoring needs to be.
2. **Interoperability** – The Digital Twin needs to "talk" smoothly with other systems, sensors, and software using standard formats and protocols. This lets it pull in data from various sources (like building systems, weather stations, or maintenance logs) and share insights with other tools too.
3. **Connectivity** – All machines, sensors, and devices in the plant need to be linked together through a strong, reliable network—one that can handle large data flows and keep communication secure.
4. **Security** – Since Digital Twins handle sensitive operational data, they need strong cybersecurity: things like network segmentation, access controls, encryption, and regular security checks to guard against breaches.
5. **Synchronization** – This keeps the digital model matched with real-world conditions at all times, so the virtual twin always reflects what's actually happening on the ground.

A good Digital Twin isn't just a digital copy—it needs to be accurate, connected, secure, and constantly in sync with the real asset to actually be useful.

## Key Components of Digital Twins




## Technology behind Digital Twins

Four core building blocks enable Digital Twins to work effectively:

1. **IoT Sensors:** Collect real-time data from physical systems and continuously update the digital twin.
2. **Data Integration:** Middleware collects, processes, and connects data from different sources, allowing the systems to communicate smoothly.
3. **AI and Machine Learning:** Analyze data and identify patterns to make predictions and support better operational decisions.
4. **Cloud and Edge Computing:** Cloud platforms provide large-scale data storage and processing, while edge computing processes data closer to the source for faster, real-time responses.

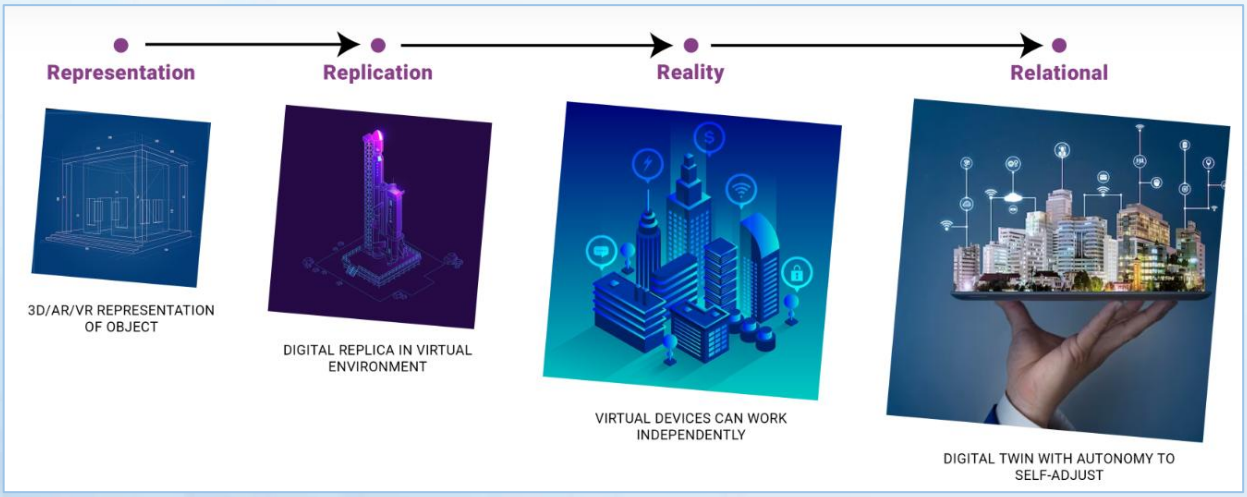
## Benefits of Digital Twin Technology

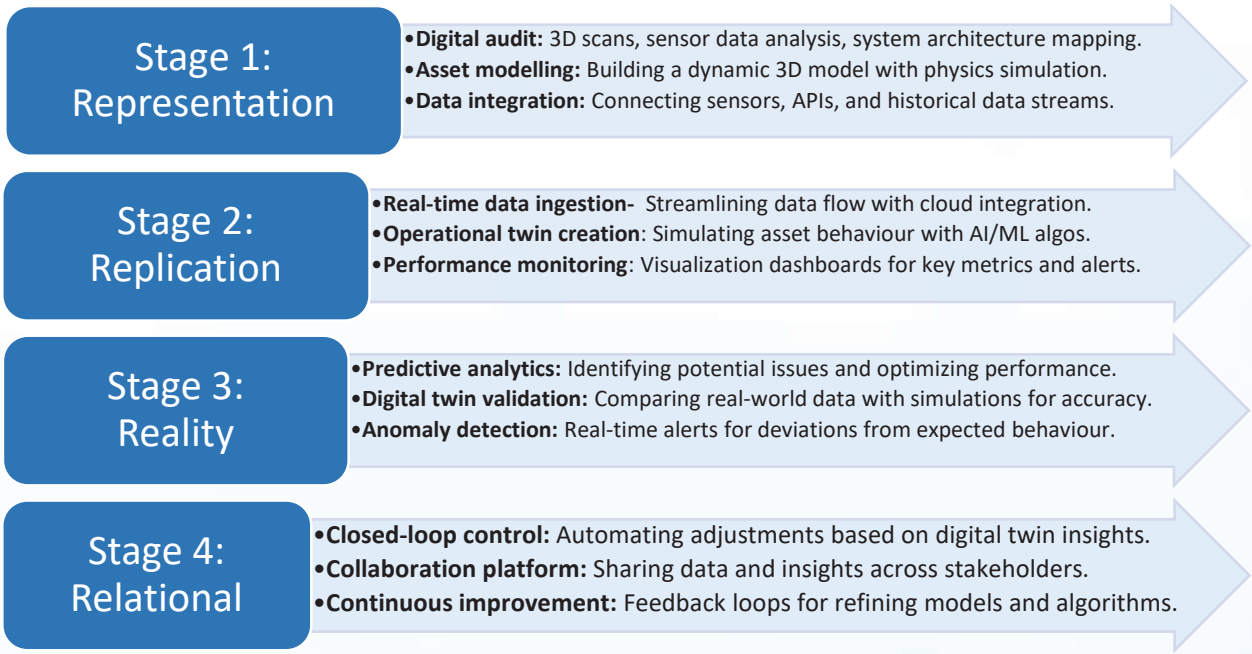
1. **Enhanced Efficiency:** Operations can be tested and optimized virtually, helping improve energy use, maintenance, and overall reliability.
2. **Cost Reduction:** Predictive maintenance can reduce downtime and repair costs, while virtual testing can lower design and development expenses.
3. **Real-Time Monitoring:** Provides a live view of system performance, allowing issues to be identified and addressed quickly.
4. **Sustainability:** Helps organizations use resources more efficiently and supports efforts to meet energy and emission targets.

## Challenges and Limitations

1. **High Initial Costs:** Setting up sensors, data platforms, connectivity, and analytics systems can require significant investment.
2. **Data Security and Privacy:** Connected devices and cloud-based systems can be exposed to cyber threats, making strong data protection essential.
3. **Complex Implementation:** Digital Twins require expertise in areas such as IoT, AI, data management, and cloud computing. Bringing these technologies together can be technically challenging.
4. **Scalability Issues:** Large-scale Digital Twins, such as those used for cities, transportation networks, or energy grids, generate huge amounts of data and require considerable computing and storage capacity.

## Stages of Digital Twins






## Digital Twin Market in India: Growth story

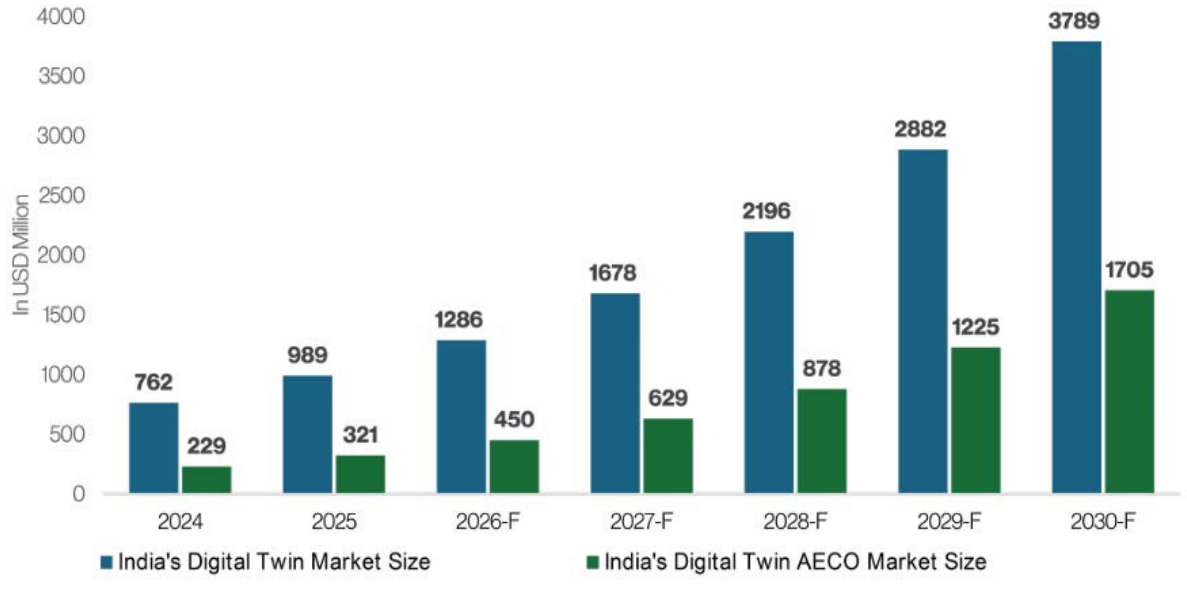
India's Digital Twin market is moving from small pilot projects to real, large-scale use in sectors like transport, utilities, and city development.

**The Big Picture:** The market is growing fast—expected to roughly grow 5x between 2024 and 2030, driven by strong demand across sectors.

**Why Construction & Real Estate (AECO) Will Lead the Way:** The Architecture, Engineering, Construction, and Operations (AECO) sector is set to become one of the biggest users of Digital Twin technology in India, with its share of the market growing significantly by 2030. Three main reasons are driving this:

1. **Infrastructure upgrades** – As India invests heavily in transport, industrial zones, and city redevelopment, Digital Twins help monitor these assets in real time and catch maintenance issues early.
2. **Better tech integration** – Building Information Modelling (BIM) is increasingly working hand-in-hand with IoT sensors and Digital Twins, enabling more accurate simulations of things like energy use and building performance.
3. **Sustainability push** – Companies are using Digital Twins to cut costs, reduce energy waste, and lower their carbon footprint.

By 2030, construction and real estate will be one of the biggest growth areas for Digital Twin technology in India, growing much faster than the market as a whole—signaling a major shift in how India builds and manages its infrastructure.

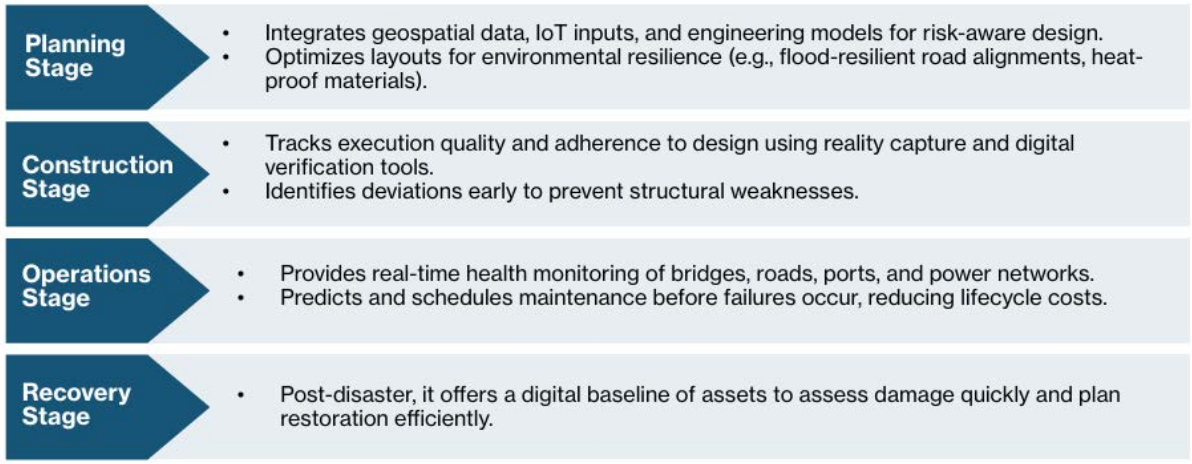



**Source:** Geospatial World Consulting Analysis

**Why Resilient Infrastructure needs Digital Twins**

- Digital Twins create a live, virtual copy of infrastructure, combining engineering, operations, and environmental data in one place.
- They let planners test out worst-case scenarios—like floods, earthquakes, heatwaves, or traffic overloads—before they actually happen, helping spot weak points in design or operations early.
- With constant monitoring, Digital Twins can flag potential equipment or structural problems before they turn into major failures, cutting downtime and preventing disasters.
- Real-time data means faster response during disruptions, helping keep services running smoothly even when things go wrong.

Digital Twins help infrastructure prepare for problems before they happen—making systems safer, stronger, and more reliable.




**Source:** Geospatial World Consulting Analysis

## Examples of Digital Twins in Indian Infrastructure

**Hyderabad Airport:** Rajiv Gandhi International Airport uses an **AI-powered Digital Twin** to integrate real-time data from airside, landside and terminal operations for predictive and efficient airport management. (GMR Group)

**Varanasi (Kashi):** A **3D Urban Spatial Digital Twin** covering around 160 sq. km. has been developed using LiDAR, GIS, aerial surveys and 3D modelling to support urban planning, traffic management and disaster preparedness. (The Times of India)

**Indian Railways:** Indian Railways explored a **Digital Twin of railway corridors** to replicate real-time train movements and simulate the impact of advanced signalling systems before implementation. (The Indian Express)

**Sangam: Digital Twin:** The **Department of Telecommunications (DoT)** launched the *Sangam: Digital Twin* initiative to explore AI-driven Digital Twins for integrated infrastructure planning, simulation and optimisation across sectors. (dot.gov.in)

## Conclusion

India's infrastructure ambitions have never been in doubt—the scale of investment, the reach of programmes like PM GatiShakti, and the sheer pace of construction all point to a country serious about its 2047 goals. What's changing now is *how* that infrastructure gets built and managed. Digital Twins represent a genuine shift in mindset: instead of finding out something doesn't work after it's built, planners can find out beforehand, in a virtual space, where mistakes are cheap and fixable.

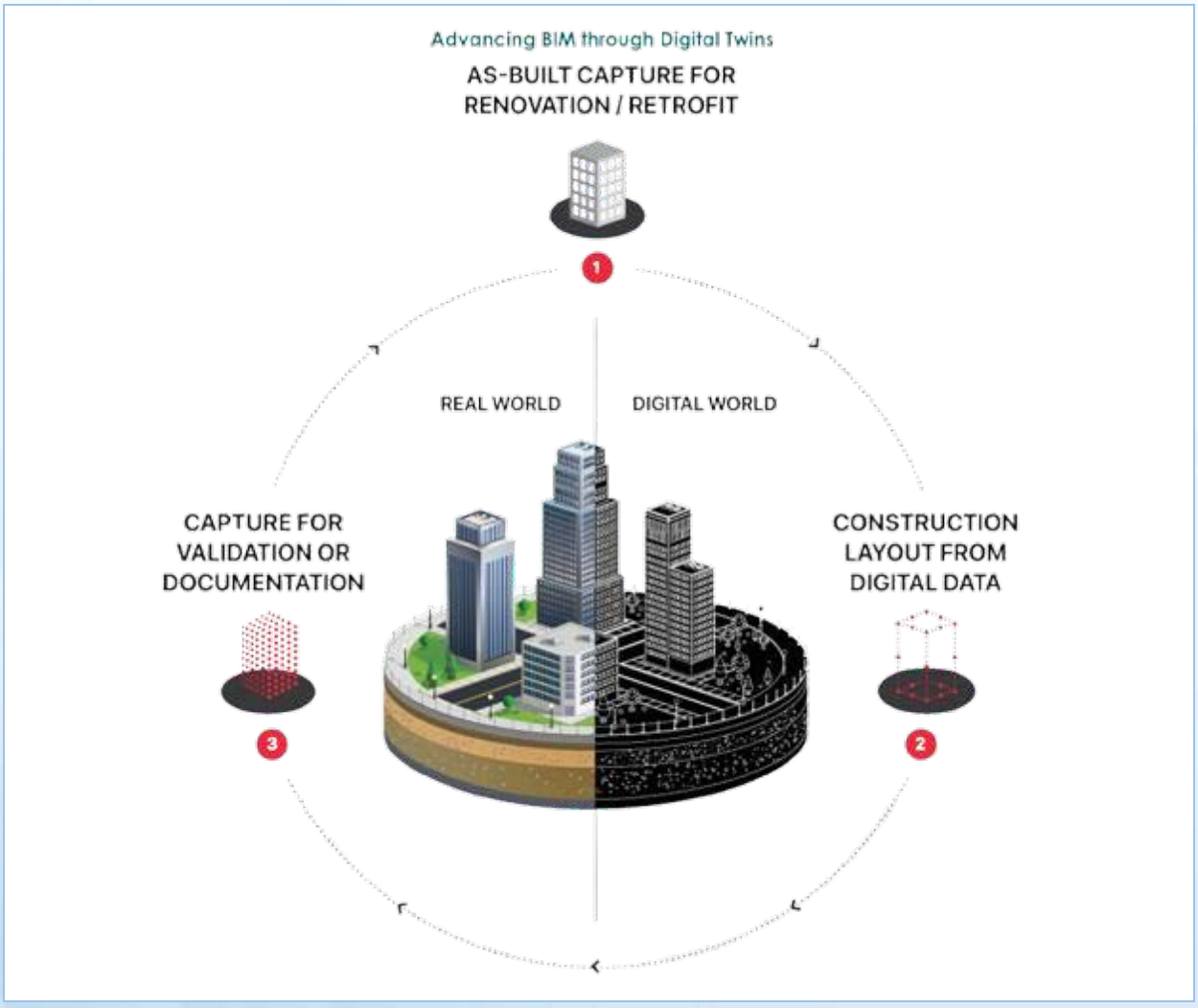
The early signs are encouraging. Hyderabad's airport, Varanasi's urban twin, and the Railways' signalling simulations aren't just proof-of-concept exercises—they're working examples of what happens when physical and digital infrastructure genuinely talk to each other. And the market

numbers back this up: a technology once confined to manufacturing floors is now becoming a serious tool for national infrastructure planning.

That said, none of this happens automatically. The same execution gaps that have long troubled Indian infrastructure—cost overruns, fragmented planning, slow environmental clearances—don't disappear just because a Digital Twin is layered on top. If anything, they need to be fixed in parallel. Technology can't paper over weak coordination between ministries or a shortage of skilled people who know how to run these systems.

India has the ambition, the early use cases, and a fast-growing market for Digital Twin technology. What it needs now is the institutional muscle to scale it responsibly.

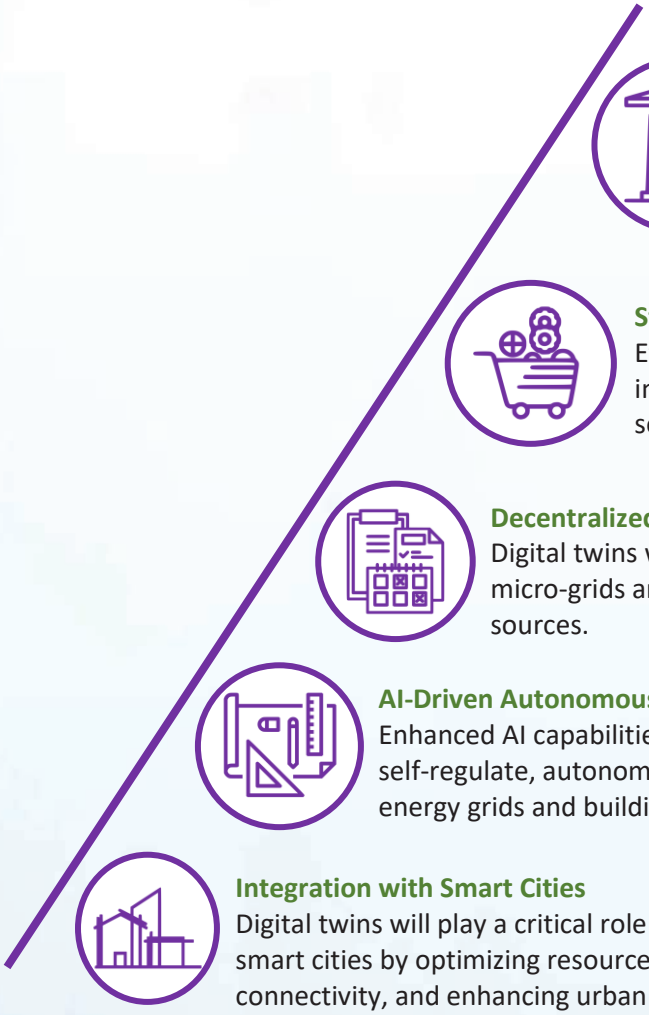
Infrastructure has always been judged by what gets physically built—kilometres of road, megawatts of power. But increasingly, India's edge will come from something less visible: how intelligently that infrastructure is planned, monitored, and adapted over time. Digital Twins won't replace the hard work of laying concrete and steel, but they can make sure that work counts for more.



## References

1. https://www.arcweb.com/industry-best-practices/digital-twin-industry-infrastructure
2. Autodesk. (n.d.). What is a digital twin? https://www.autodesk.com/design-make/articles/what-is-a-digital-twin
3. Economic Times Government. (2023, October 11). PM GatiShakti National Master Plan: Digitally enabled roadmap for innovative infrastructure. https://government.economictimes.indiatimes.com/blog/pm-gatishakti-national master-plan-digitally-enabled-roadmap-for-innovative-infrastructure/115903478
4. EY India. (n.d.). Digital twins: Creating intelligent industries. https://www.ey.com/en_in/insights/technology/digital twins-creating-intelligent-industries
5. Fortune Business Insights. (n.d.). Digital twin market size, share & trends report. https://www.fortunebusinessinsights.com/digital-twin-market-106246
6. Geospatial World. (2023, March 14). India: Real-time digital twins & predictive AI. https://geospatialworld.net/artha/ interview-artha/india-real-time-digital-twins-predictive-ai/
7. Digital Twin Market size, Share & Industry Analysis. Online: https://www.fortunebusinessinsights.com/digital-twin-market-106246 4.
8. Gartner Research Emerging Technologies: Revenue Opportunity Projection of Digital Twins. Online: https://www.gartner.com/en/documents/4011590 5.
9. India Digital Twin Market Research Report: https://www.marketresearchfuture.com/reports/india-digital-twin-market 21441#download.pdf.

## Future Trends



**Extended Reality (XR) Integration**
Combining digital twins with AR/VR for immersive visualizations will redefine design, planning, and training processes.

**Standardization and Interoperability**
Efforts to standardize digital twin platforms will improve adoption across industries and enable seamless integration.

**Decentralized Energy Systems**
Digital twins will enable efficient management of micro-grids and decentralized renewable energy sources.

**AI-Driven Autonomous Systems**
Enhanced AI capabilities will allow digital twins to self-regulate, autonomously optimizing systems like energy grids and building management.

**Integration with Smart Cities**
Digital twins will play a critical role in managing smart cities by optimizing resources, improving connectivity, and enhancing urban living.



# OUR CONTRIBUTORS

# OUR CONTRIBUTORS



## From Identity to Inclusion: How India Built Digital Public Infrastructure as an Enabler of Inclusive Governance

**Aashita Dagar, India**

Aashita Dagar is a Techno-Business leader with 26 years of experience translating technology capabilities into sustainable business growth, bringing a global perspective from delivery for customers across the US, UK and India. Currently Principal Consultant with the Emerging Technology & Digital Transformation team at NeGD (MeitY), she is part of the AI team working with the IndiaAI Mission and led the national AI/ML RFE empanelment on CPPP as Convener. A veteran of TCS, Infosys and Coforge, she has delivered large-scale digital transformation programmes for national platforms including UIDAI, DoP and NHA, and closed deals exceeding USD 150M+.

## How Digital Systems Become Public Infrastructure: DPI Transformability and the Institutional Conversion of Digital Public Infrastructure



**Kentaro Saito, Japan**

Kentaro Saito currently serves as Deputy Director of the Office of International Affairs at the Board of Audit of Japan. During his more than 20 years with the Board, he has spent approximately half of his career working in the Office and the Research Division, gaining extensive experience in these areas. Drawing on his knowledge and expertise, he has represented the Board at a large number of INTOSAI and ASOSAI meetings. He is also a member of the Board's IT Audit Skills Development Team where he contributes to the Board's digital audit initiatives. He holds Master in Development Economics from SOAS, University of London and Master in Labour Economics and Human Resources from Le Mans University.



## Digital Public Infrastructure as an Enabler of Inclusive Governance: Mechanisms, Evidence, and the Audit Imperative

**Harsha Bhowmick, India**

Harsha Bhowmick is Director of Digital Economy and Fintech at the Government of India, with over 22 years of experience in fintech, financial inclusion and digital transformation. His work spans digital payments, KYC, MSME lending, open data and the globalisation of Digital Public Infrastructure (DPI). In his current role, he supports G20 priorities through the Financial Inclusion Working Group, fostering global partnerships and contributing to policy deliberations. He has expertise in financial advisory and microfinancing and has led initiatives promoting digital financial inclusion and India's digital economy. A speaker and guest lecturer, he regularly participates in national and international panel discussions, fireside chats and keynote sessions. Previously, he led a management consulting practice, overseeing financial targets and strategic delivery, and worked on product strategy, digital transformation and system design. He has expertise in emerging technologies including AI/ML, blockchain, RPA and IoT.

## Digital Public Infrastructure as an Enabler of Inclusive Governance: Mechanisms, Evidence, and the Audit Imperative

**Abhishek Singh, India**



Abhishek Singh is an officer of SAI India, currently serving as Director (Training & Research) at the International Centre for Information Systems & Audit (iCISA), the global capacity building centre of SAI India and Global Training Facility of WGITA. An engineering graduate, he brings extensive experience in IT Audit, Data Analytics, Performance, Compliance and UN Audit, including international assignments with the Organisation for the Prohibition of Chemical Weapons (OPCW), The Hague. At iCISA, he steers international training programmes on emerging audit themes such as e-Procurement, Public-Private Partnerships, Digital Public Infrastructure etc and has contributed to the Global Certification Course on Data Science, AI/ML and Cybersecurity Audit with IIT Madras. He is closely associated with iCISA's strategic transformation roadmap, AI-enabled multilingual training, and partnerships with Supreme Audit Institutions worldwide.



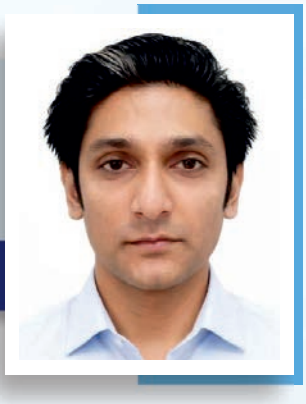
## From India Stack to Citizen Stack: India's DPI Journey and a Blueprint for the World

**Karan Vohra, India**

Karan Vohra is an Indian Audit and Accounts Service (IA&AS) officer of the 2016 batch. He has varied experience across the department, having served in the O/o PAG (Audit-I), Maharashtra, and in the Centre for Data Management and Analytics (CDMA) and the International Relations Wing at the CAG headquarters; he is currently posted as Director in the Office of the Director General of Audit (Central Expenditure), New Delhi. He holds a Bachelor of Engineering degree from Thapar University, Patiala, and was conferred the CAG Award for Innovation and Excellence in Public Sector Auditing and Accounting in 2021.

## From India Stack to Citizen Stack: India's DPI Journey and a Blueprint for the World

**Keshav Bhardwaj, India**



Keshav Bhardwaj is a Research Associate at the Indian Institute of Management's Center for Digital Public Goods (CDPG), where he works on various projects relating to research, documentation, and implementation of Digital Public Infrastructure (DPI) and Digital Public Goods (DPG). He holds Bachelor's and Master's degrees from Banaras Hindu University, and has previously served as a Young Professional in the International Relations Division of the Office of the Comptroller & Auditor General of India (SAI India).



## Mapping Municipal Equity: Leveraging Spatial DPI for Inclusive Solid Waste and Utility Management in Smart Cities

**Dr. Nanda Dulal Das, India**

Dr. Nanda Dulal Das, Director, NAAA, is a civil servant belonging to the Indian Audit and Accounts Service (IA&AS) of 2015 batch, currently serving as Director at the National Academy of Audit and Accounts (NAAA), Shimla, India (the premier training ground for the IA&AS cadre). He holds a Ph.D. specialising in spatial convergence modelling between rural employment guarantee programmes and watershed development programmes in India, remote sensing, and GIS applications, an M.Phil., M.Com. and a M.A. degree. Dr. Das also conducted a nine-month long post-doctoral research on municipal solid waste lifecycles and smart city utility rate structures. He enjoys teaching and regularly teaches commercial auditing concepts, financial management, Information Systems Audit, environmental audit and other important tools used in public sector auditing in NAAA.

## Auditing the Connectivity Layer of Digital Public Infrastructure: Lessons from BPK's Performance Audit of the Indonesian Telecommunications Infrastructure Regulatory Agency

**Benidiktus Bambang Triasmoro, Indonesia**



Benidiktus Bambang Triasmoro is an audit team leader at the Audit Board of the Republic of Indonesia (BPK). He holds a bachelor's degree in computer science and a master's degree in information technology. Since 2019 he has audited the Ministry of Communication and Digital Affairs. He currently leads a performance audit of Indonesia's national data-centre ecosystem, applying the WGITA–IDI Handbook on IT Audit (2022). His professional interests include IT performance audit, data-centre governance, and digital public infrastructure.



## Auditing the Connectivity Layer of Digital Public Infrastructure: Lessons from BPK's Performance Audit of the Indonesian Telecommunications Infrastructure Regulatory Agency

**Dwi Jatmika Bima Mahatmantara, Indonesia**

Dwi Jatmika Bima is an Auditor of the Audit Board of the Republic of Indonesia (BPK). He holds a bachelor degree in Accounting and experienced in government audit for 16 years. Recently conducted IT-related performance audit at the Indonesian Ministry of Communication and Digital Affairs as a sub team leader, those are:

- The Effectiveness of the Provision and Utilization of Information and Communication Technology (ICT) Infrastructure in Support of Digital Transformation
- The Effectiveness of Activities to Prevent the Dissemination of Content Prohibited by Laws and Regulations in the Operation of Electronic Systems and Transactions
- The Effectiveness of Expenditure Management in the Provision of Infrastructure and Telecommunication Services
- The Effectiveness of the Management of the National Data Center Ecosystem

## Auditing the Connectivity Layer of Digital Public Infrastructure: Lessons from BPK's Performance Audit of the Indonesian Telecommunications Infrastructure Regulatory Agency

**Arief Ridhatama, Indonesia**



Arief Ridhatama has enrolled as an Auditor of the Audit Board of the Republic of Indonesia (BPK) since 2020. He holds a bachelor degree in Accounting and then pursuing postgraduate degree in Environmental and Natural Resource Economics in University of Birmingham. Since 2020 he has conducted financial, performance, and compliance audit on the Ministry of Communication and Digital Affairs, then at 2025 has finished the performance audit in Spectrum Management and 2026 done Financial Audit of financial report of year 2025, both as a team leader.

Recently, he became second in lead on a performance audit of Indonesia's national data-centre ecosystem.



## Auditing the Connectivity Layer of Digital Public Infrastructure: Lessons from BPK's Performance Audit of the Indonesian Telecommunications Infrastructure Regulatory Agency

**Achmad Faishal, Indonesia**

Achmad Faishal is Deputy Director of Audit III.C.1 at the Audit Board of the Republic of Indonesia (BPK), within the Directorate General of Audit III. He holds a bachelor's degree in economics and a master's degree in management. He oversees audits of the Ministry of Communication and Digital Affairs, covering the management and accountability of state finances, including digital infrastructure and public information systems. His professional interests include public-sector audit, digital government, and the governance of national digital ecosystems.

## Auditing the Connectivity Layer of Digital Public Infrastructure: Lessons from BPK's Performance Audit of the Indonesian Telecommunications Infrastructure Regulatory Agency

**Amri Lewa, Indonesia**



Amri Lewa is Director of Audit III.C at the Audit Board of the Republic of Indonesia (BPK), within the Directorate General of Audit III. He holds a bachelor's degree in accounting and a master's degree in advanced accounting, and is a chartered accountant. He directs audits of government entities under his portfolio, including the Ministry of Communication and Digital Affairs. His responsibilities cover financial, performance, and information-technology related audits of state financial management. His professional interests include public-sector auditing, digital government accountability, and IT audit practice.

## Digital Public Infrastructure and Cloud Computing: GAO Identified Challenges

**Jonnie Genova, USA**



Jonnie Genova is Communications Analysts at the U.S. Government Accountability Office (GAO), where she supports auditors in developing written products for GAO's Information Technology and Cybersecurity Team.



## Digital Public Infrastructure and Cloud Computing: GAO Identified Challenges

**Jess Lionne, USA**

Jess Lionne is Communications Analysts at the U.S. Government Accountability Office (GAO), where she supports auditors in developing written products for GAO's Information Technology and Cybersecurity Team.

## AgniDrishti: An AI-Enabled Fire Risk Intelligence System as Digital Public Infrastructure for India's Fire and Emergency Services

Tania Mishra, India



Tania Mishra is an IA&AS Probationer (2024 Batch) currently undergoing training at the National Academy of Audit and Accounts, Shimla, and posted at the Office of the Principal Accountant General (Audit-I), Kolkata. During field posting she conducted a pilot Subject Specific Compliance Audit of the West Bengal Fire and Emergency Services (2023-26), during which she developed AgniDrishti, an AI-assisted fire risk analysis prototype. She is the author of "Biometric Systems and the Problem of Usability: A Governance-Centric Intervention in Attendance Management," published in Manthan: Journal of Public Sector Auditing and Accounting of SAI India (Volume 1, Issue 2, May 2026), a peer-reviewed journal of the Indian Audit and Accounts Department published by the National Academy of Audit and Accounts, Shimla.



## Digital Public Infrastructure for Inclusive Governance: The EASE Platform for Citizen-Centric Entitlement Services in Jharkhand, India

Bhargav Ram Khyathi, India

Bhargav Ram Khyathi is a 2023-batch officer of the Indian Audit and Accounts Service, currently serving as Deputy Accountant General in the Office of the Principal Accountant General (A&E), Jharkhand. He graduated in Computer Engineering from Netaji Subhas Institute of Technology, Delhi, and, prior to joining the civil services, worked as a software developer with Google, Hyderabad, and Samsung Research Institute, Noida. His professional interests include artificial intelligence, data analytics, digital transformation and their application in public financial management, government accounting and audit.

## Who Benefits from Digital Public Infrastructure? Auditing Inclusion, Accountability, and Service Delivery Outcomes

**Maha Fathy Ibrahim Morsy, Egypt**



Maha Fathy has 16 years of experience with the Accountability State Authority of Egypt, specialising in public-sector auditing and auditing international organisations, including UNIDO, UN Tourism, and several African Union organisations. She holds a Master's degree in Auditing from Cairo University. She is a member of ASA teams participating in international and regional working groups, including the INTOSAI Working Group on IT Audit (WGITA) and the ARABOSAI IT Audit Working Group. Her professional interests include artificial intelligence, IT auditing, data analytics, and emerging technologies.



## From AI Access to Ethical Readiness: Auditing AI-Enabled Education DPI for Inclusive Governance Reflections from India Stack and Uzbekistan's Emerging Experience

**Rustamkhuja Ishanov, Uzbekistan**

Rustamkhuja Ishanov holds a Master's in Public Administration from Uzbekistan's Academy of Public Administration, with further degrees in jurisprudence, economics and English philology. With over twenty years in public service and digital governance, he currently serves as Head of Department at UZINFOCOM LLC, Uzbekistan's single integrator for state information systems. His work focuses on digitalisation, IT governance, AI ethics, project management and data analysis. He participated in the 166th International Training Programme on Audit of Digital Public Infrastructure at iCISA.

## Diagnosing and opening the black-box of Digital Public Infrastructure: A Process-Audit Approach to Inclusive Governance

**Chakradhar Buddha, India**



Chakradhar Buddha is a transparency and accountability activist and co-founder of LibTech India. He has extensive experience working on land rights, Adivasi rights and social protection. His work focuses on how technology and digital systems affect people's access to rights and entitlements, particularly in rural and tribal areas. He has been involved in field-based research and policy engagement on rural employment, social security and digital land governance. He has authored a book in Telugu, a major Indian language, on India's rural employment guarantee programme, MGNREGA, and regularly contributes to the media on social protection, digital governance and Adivasi rights



## Diagnosing and opening the black-box of Digital Public Infrastructure: A Process-Audit Approach to Inclusive Governance

**Dr. Rajendran Narayanan, India**

Dr. Rajendran Narayanan teaches in the School of Humanities and Social Sciences at Azim Premji University, Bangalore. After completing his PhD in statistics from Cornell University, Rajendran has held academic positions in Indian Statistical Institute, Kolkata, Cornell University and Ashoka University. He is also a founding member of LibTech India, an organisation that works to improve transparency and accountability of rural social policies in India. He has authored several research papers, book chapters and reports. Recently, he co-edited a Handbook of Welfare in India titled 'Realising Rights.' He contributes regularly in English and Hindi in the popular media.

## Inclusion by Verification: Why Digital Public Infrastructure's Promise of Inclusive Governance Depends on a Dedicated Data-Reliability Audit Approach

Jishnu J Raju, India



Jishnu J Raju is a Deputy Director in the Capacity Building Wing of the Office of the Comptroller and Auditor General of India, where he works on institutional capacity building, competency development and emerging technology initiatives for public-sector auditing. His responsibilities include developing training strategies, competency frameworks and digital learning programmes, and coordinating partnerships with leading academic and technology institutions. He has been closely associated with initiatives relating to Digital Public Infrastructure, data science, artificial intelligence, machine learning, cyber-security and digital systems audit. His professional interests include the implications of large-scale digital transformation for public accountability, audit methodologies and institutional capability. Through his work, he engages with the evolving challenges of auditing technology-enabled governance and strengthening the readiness of Supreme Audit Institutions for the digital public sector. He has also prior experience working with the central bank of India.



## Extending the Use of Audit Data Can Help Strengthen Inclusivity

Sandeep Radhakrishnan, India

Sandeep Radhakrishnan is a Senior Associate at Artha Global at their Centre for Technology and Innovation. With a background in economics, he has held positions in consulting, civil society, and finance. The majority of his experience has been within the digital economy field, where he has worked on numerous policy and advocacy issues related to personal data rights, fair competition, governance structures, etc. He also has experience as a climate and sustainability consultant, wherein he advised large corporates on their transition to net-zero emissions and worked with venture capital firms to help structure their ESG portfolios. He has completed his BSc and MSc from the universities of Essex and Nottingham, respectively.

## Auditing Digital Public Infrastructure for Inclusive Governance: Insights from India's Direct Benefit Transfer Experience

Sameer Asif, India



Sameer Asif is currently working as Assistant Audit Officer in AMG-III section of O/o PDA ICA New Delhi since September 2022. He has a keen interest in IT and related systems. He was part of thematic Audit of RMDP Nepa Limited, Performance Audit of FAME India Scheme, and is currently engaged in Performance Audit of Nation Industrial Corridor Development Programme (NICDP).



## Auditing Decision Accountability in AI-Enabled DPI: Lessons from a Social Impact Study of Welfare Schemes in India

Bijay Kumar Mohanty, India

Bijay Kumar Mohanty is a part of Senior Management of SAI India and has more than three decades of distinguished service across Headquarters, State Audit, Railways and international organizations. He is currently serving as Director General iCISA, ADAI (Capacity Building & IS) & CTO in the Office of the Comptroller & Auditor General of India. He is actively involved in digital transformation of the department by leading a data driven audit framework. He is responsible for implementing the AI strategy of the department and is heading the sovereign audit LLM project and creating AI agents for giving assurances on public sector IT Applications. He is pioneering the cybersecurity audit aimed at assuring the government about security resilience of mission critical applications.

He has represented India in several important global engagements, including the SAI20 Summit 2025 in South Africa; meetings of EUROSAI ITWG and the Working Group on Big Data.

## Auditing Decision Accountability in AI-Enabled DPI: Lessons from a Social Impact Study of Welfare Schemes in India

Krishnan Narayanan, India



Krishnan Narayanan is co-founder and President of itihaasa Research and Digital, where he studies the evolution of emerging technologies and innovation. He is the co-author of the award-winning Against All Odds: The IT Story of India (2022), Empowering India (2023), The Co-Intelligence Revolution (2025), and Co-Creating the Future with AI (2026). He is a founding board member of AquaMAP, a national centre for water management and policy, and an advisor to the Global Learning Council, Switzerland. He also teaches and conducts research at IIT Madras, including at its Centre for Responsible AI. Krishnan holds degrees from IIT Madras and XLRI Jamshedpur.



## Auditing Decision Accountability in AI-Enabled DPI: Lessons from a Social Impact Study of Welfare Schemes in India

V.R. Muraleedharan, India

V. R. Muraleedharan is Professor Emeritus in the Department of Humanities and Social Sciences and the head of the Centre for Technology and Policy at IIT Madras. He is a development economist with longstanding interests in healthcare economics, technology and health policy, and universal health coverage. He has taught at IIT Madras since 1988 and has held several academic leadership and policy-advisory roles. His scholarship includes numerous journal articles, research monographs and policy reports, as well as the co-authored book The Challenge of Health Sector Reform: What Should Governments Do? His work bridges academic research and public policy, with sustained engagement in health-system strengthening in India.

## Auditing Digital Public Infrastructure: Strengthening Inclusive Governance through Supreme Audit Institutions

Serah Kituu, Kenya



Serah Kituu (SAI Kenya) is a Principal Auditor in the Public Service and ICT Audit Directorate at the Office of the Auditor-General (OAG), Kenya, with over 11 years of experience in public-sector auditing. Previously, she served in the Systems Assurance and Data Science Directorate, specialising in IT assurance and data analytics. She has conducted information systems audits across ministries, state corporations, county governments, public universities, and the health sector. She contributed to the development of SAI Kenya's IS Audit Manual and championed the implementation of TeamMate+. She holds an MBA from the University of Nairobi and a Bachelor's degree in Computer Applications from Periyar University.



## Beyond IS Audit: Auditing the Invisible Architecture of Digital Public Infrastructure

Ajay Yeshwanth, India

Ajay Yeshwanth is Director (Information Systems) at the Office of the Comptroller and Auditor General of India, where he leads strategic initiatives in technology audit, digital transformation, and institutional capacity building. He headed the team that prepared the Digital Public Infrastructure (DPI) Audit Guidelines for SAI India. He holds a Master's in Public Administration from the Lee Kuan Yew School of Public Policy, National University of Singapore, and a Bachelor's in Production Engineering from National Institute of Technology, Tiruchirappalli.

## Digital Public Infrastructure as an Enabler of Inclusive Governance: Opportunities, Risks, and the Role of Audit

**Pranay Chauhan, India**



Pranay Chauhan is a leading Cybersecurity and GRC Expert with 18+ years of specialized experience in IT audit, GRC (Governance, Risk & Compliance), and system audits. He holds advanced credentials including ISO 27001/42001 Lead Auditor, and PCI-DSS 4.0, complemented by M.E. IT with Distinction. Currently serving as vCISO and cyber security consultant, he specializes in incident response, blockchain technology, and AI security. As faculty at ICAI's Digital Accounting and Assurance Board (DAAB). he contributes to professional standards in digital audit and compliance. His work spans government and private sector engagements across India.



## Auditing Digital Public Infrastructure: Lessons from TCU (SAI Brazil) on Quality Assessment of Selected Federal Digital Services

**André Luiz de Albuquerque Farias, Brazil**

André Luiz de Albuquerque Farias is a senior infrastructure professional with 15 years of experience in governance, public policy, regulation, and infrastructure project structuring. He currently serves as Director of Airport Infrastructure and Civil Aviation Affairs at Brazil's Federal Court of Accounts (SAI Brazil), where he leads the team responsible for overseeing airport concessions and the performance of public-private partnerships, regulatory compliance, and policy oversight. He also serves as an expert adviser on contract renegotiations in the infrastructure sector.

## Digital Public Infrastructure as an Enabler for Inclusive Governance

Malik Sulaiman Hamood Al Ghawi, Oman



Malik Sulaiman Hamood Al Ghawi specialises in Network and Computer Engineering. He began his career as a Network Engineer at Huawei before joining the State Audit Institution of the Sultanate of Oman. He is certified in cybersecurity by (ISC2) and is a member of the (ISC2) Oman Chapter. He also holds certifications in cybersecurity and artificial intelligence, as well as several certifications in data science, machine learning, Python programming, geographic design, website development, mobile applications, networking and other related fields.



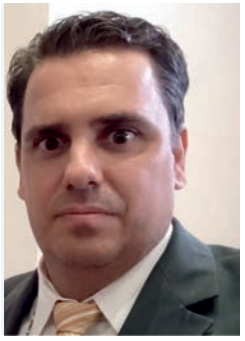
## Auditing Digital Public Infrastructure During Implementation: Lessons from Brazil's Gestão Presente System (SGP)

Klauss Nogueira, Brazil

Klauss Nogueira is a Federal Auditor for External Control at the Federal Court of Accounts of Brazil (TCU), with experience in information technology and public-sector auditing. His work focuses on IT audit, digital transformation, artificial intelligence, transparency, and citizen-centered public auditing. He has contributed to initiatives aimed at incorporating citizens' perspectives into public-sector oversight and has authored and co-authored articles on technology, transparency, citizen participation, and innovation in public auditing, including publications in the INTOSAI Journal.

## Auditing Digital Public Infrastructure During Implementation: Lessons from Brazil's Gestão Presente System (SGP)

Fernando Faria, Brazil



Fernando Pereira de Faria is a Federal Auditor for External Control at the Federal Court of Accounts of Brazil (TCU), specializing in IT audit with a focus on data and systems. His work centers on the oversight, architecture, and governance of cloud environments, with particular emphasis on platforms such as AWS and Azure, as well as digital transformation and innovation in public sector auditing. He has authored and co-authored articles and technical papers on technology, data governance, cloud infrastructure, and innovation in public-sector oversight.



## Auditing Digital Public Infrastructure During Implementation: Lessons from Brazil's Gestão Presente System (SGP)

Harley Ferreira, Brazil

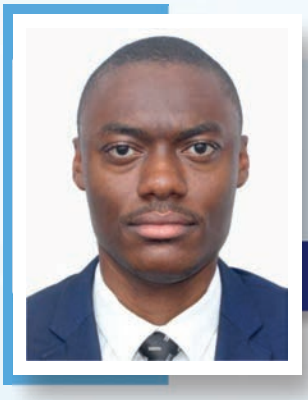
Harley Alves Ferreira is a Federal Auditor for External Control at the Federal Court of Accounts of Brazil (TCU), with over 22 years of experience in information technology auditing. He holds a bachelor's degree in computer science and is a Certified Information Systems Auditor (CISA) and member of ISACA. He currently serves as an Advisor at TCU's Secretariat for Information Technology Oversight and works in various areas related to information technology auditing. He has extensive professional experience, having previously served as an Air Traffic Controller, Analyst at the Central Bank of Brazil, Federal Revenue Auditor, and Federal Criminal Expert.

## Auditing Digital Public Infrastructure During Implementation: Lessons from Brazil's Gestão Presente System (SGP)

**Rafael Albuquerque, Brazil**



Rafael Albuquerque da Silva is a Federal Auditor for External Control at the Federal Court of Accounts of Brazil (TCU) and serves as Chief Auditor of the Information Technology Audit Unit. He holds a degree in Computer Science and a postgraduate specialization in IT Governance. His work focuses on IT governance, digital transformation, data governance, and the use of data to improve public policies. He is particularly interested in strengthening government capabilities to promote data-driven decision-making, improve information quality, and advance digital government with transparency, security, accountability, and a strong citizen-centered approach.



## Digital Public Infrastructure as an Enabler of Inclusive Governance: An Audit Perspective from Sierra Leone

**Abu Allicious Gogra-Hilton, Sierra Leone**

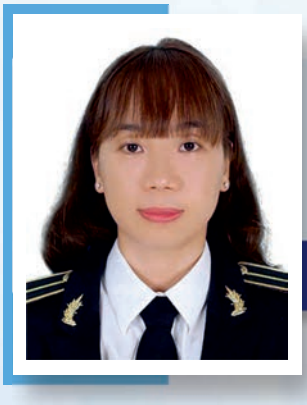
Abu Allicious Gogra-Hilton is an Auditor in the General Accounts Division of the Audit Service Sierra Leone (ASSL), Freetown, where he specializes in conducting financial and compliance audits on Ministries, Department and Agencies. He is concurrently pursuing a Master of Auditing (MAud) at the School of Government Audit, Nanjing Audit University, China. His research centers on big data audit implementation in Sierra Leone. His professional interests include information systems audit, public sector governance reform, and digital accountability frameworks for developing economies.

## The Technological Crossroads: Challenges and opportunities of Digital Public Infrastructure in Cuba



**Makisleidis Esponda Bravo, Cuba**

Makisleidis Esponda Bravo has over 15 years of professional experience, primarily with Cuba's Ministry of Foreign Trade and Investment (MINCEX), where she has worked since 2011. She currently serves as Deputy Director of the Inspection Directorate, overseeing regulatory compliance and the control of commercial and foreign investment operations. She has completed diplomas in Foreign Trade; Management and Evaluation of Businesses with Foreign Investment; International Collaboration; and Foreign Trade, Investment and International Cooperation, along with specialised courses in e-commerce, trade, taxation, tariff classification and international cooperation. She has also participated as a speaker at international events, including the Regional Workshop on the Harmonization of E-Commerce Laws in the Caribbean, promoted by UNCTAD and other international organisations. Her research interests include e-commerce in Cuba, joint ventures and sustainable local development. She is currently pursuing a Master's degree in Local Development Project Management.



## Auditing Digital Public Infrastructure in the Age of Artificial Intelligence: A Vietnamese Perspective on Moving toward Proactive Public Audit

**Tran Thi My Giang, Vietnam**

Tran Thi My Giang is an Auditor at the State Audit Office of Vietnam. Her professional interests include public sector auditing, digital transformation in audit, data analytics, information systems audit and the use of technology to improve audit quality, efficiency and public accountability.

# Building Tomorrow, Today: How Digital Twins are reshaping India's Infrastructure journey to 2047

Piyush Tiwari, India



Piyush Tiwari is an Assistant Audit Officer (AAO) in the Data Analytics Wing, Office of the Director General of Audit (Infrastructure), New Delhi. A Computer Science Engineer, he has professional experience with Infosys and NPCI and specialises in IT audit, data analytics, data visualisation, cybersecurity, AI/ML, and emerging technologies. He previously served in the Research Wing at iCISA, Noida, contributing to national and international capacity-building programmes. He also served in Defence Commercial Audit, Bengaluru, where he was involved in IT and data-driven audits of major Defence PSUs and government entities, including HAL, BEL, BEML, MDL, GRSE, ONGC, and HSL. He holds certifications in cybersecurity, ethical hacking, and AI/ML and has completed a Data Science, AI, ML & Cyber Security certification programme from IIT Madras.

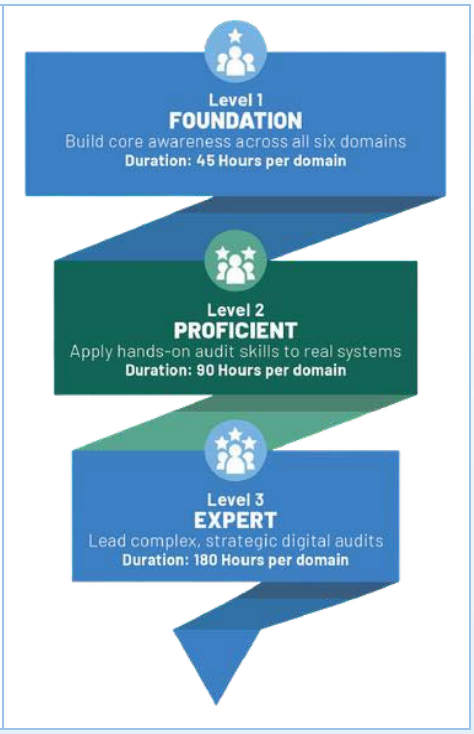


# GLOBAL CAPACITY BUILDING INITIATIVES OF SAI INDIA

# CERTIFICATION ON AUDIT OF DIGITAL SYSTEMS (CADS)

The Comptroller and Auditor General of India has, in recent years, steadily expanded its focus on digital and technology-enabled audit capability. The **Certification on Audit of Digital Systems (CADS)** marks a significant step in this effort, formalising it into a structured pathway for professional skilling. Launched by the Comptroller and Auditor General of India, Shri K. Sanjay Murthy, at the Indian Institute of Technology Madras on 27 August 2026, CADS stands as a flagship initiative within this wider programme of institutional modernisation — designed to equip auditors, in India and abroad, with the specialised capabilities that today's digital and AI-driven governance landscape demands.




CADS is structured around six domains that together cover the modern audit landscape: Information Technology Audit, Information Systems Audit, Artificial Intelligence Audit, Cybersecurity Audit, Digital Public Platforms & Privacy Audit, and Public Audit. Learners progress through three levels — Foundation, Proficient and Expert — moving from core awareness to hands-on sandbox practice on live audit problems, and finally to leading complex, strategic digital audits.

The programme is delivered through an intuitive digital learning platform and assessed through a proctored examination, with higher levels adding sandbox practice and on-site immersion. Crucially, it carries academic weight as well as professional value: every level earns credits under the National Credit Framework, counting toward the Academic Bank of Credits.

# INAUGURATION OF GLOBAL CERTIFICATION COURSE BY OFFICE OF THE C&AG OF INDIA AT IIT MADRAS ZANZIBAR

SAI India, while increasingly positioning itself as a knowledge partner for audit bodies on the global stage, has launched a new global certification course on Data Science, AI/ML and Cybersecurity Audit, delivered through the ITEC (Indian Technical and Economic Cooperation) framework in partnership with IIT Madras, bringing together thirty professionals drawn from nine African Supreme Audit Institutions.

It extends a long-running Indian tradition of technical cooperation with developing nations into the audit profession's newest frontier.






The academic anchor for this outreach is IIT Madras, notably a UN-designated Centre of Excellence on AI. What gives the partnership particular weight here is IIT Madras's own international footprint: alongside its global research standing, the institute maintains an international teaching presence that includes a campus in Zanzibar. This programme reflects India's underlying audit-technology expertise internationally through an intensive, cohort-based format. It points to an institution shaping not only its own audit practice, but the way digital and AI-era auditing capability is built more broadly across the Global South — with IIT Madras's Zanzibar presence serving as a tangible link in that ambition.






*First-ever International Training Programme (ITP) on "Audit of Digital Public Infrastructure (DPI)" conducted by iCISA under the Indian Technical and Economic Cooperation Programme.*




*Panel Discussion during the ITP on "Audit of Digital Public Infrastructure (DPI)" conducted by iCISA*

**INTERNATIONAL CENTRE FOR INFORMATION SYSTEMS & AUDIT**

A Global Capacity-Building Centre of C&AG of India

*The next issue of PursuIT will be on the theme of Cybersecurity. Details will follow.*

A-52, Sector 62, Institutional Area, Phase II, Noida - 201309, U.P. India

+91 120 240 0050 - 52, 2400049, 2400129

icisa@cag.gov.in