From DPI Strategy to Safe Scale: A Practical Implementation Framework - Revised edition 1.1, November 2026

Independent Technical Working Paper

Version 1.1 | November 22, 2026

Nasir Rehman Shaikh, Independent Advisor, AI Governance and Human Oversight, Dubai, United Arab Emirates

---

FROM DPI STRATEGY TO SAFE SCALE

A Practical Implementation Framework for Digital Infrastructure, AI Adoption and Data

www.nasirrehmanshaikh.com

Purpose

A practitioner framework for translating DPI strategy into architecture, implementation, AI adoption, data governance and measurable operational outcomes.

Status

Independent publication. Not an official publication or endorsed framework of the United Nations, UNDP or the DPI Safeguards Initiative.

Abstract

Digital Public Infrastructure succeeds when foundational systems for identity, payments and data exchange become trusted, usable and sustainable public infrastructure. The implementation challenge is not how to build a platform but how to move from strategy to safe scale while preserving interoperability, security, privacy, inclusion, accountability and long-term adoption. This working paper proposes a DPI Scale-to-Value Framework connecting strategic intent, technical architecture, data governance, AI adoption and organisational change through a seven-stage execution cycle, Align, Architect, Govern, Build, Pilot, Scale, Learn, each closed by an explicit decision gate. The paper covers strategic alignment, architecture decision records, data governance controls, progressive AI adoption as a managed capability, operating-model and change requirements, procurement as an implementation lever, pilot-to-scale evidence, a scale readiness scorecard, an implementation dashboard, and red-team failure questions. The framework deliberately complements the Universal DPI Safeguards Framework's five lifecycle stages and five implementation pathways. It is a conceptual practitioner contribution: the gates, scorecard and dashboard are proposals that

have not been empirically validated, and the central claim, that DPI should be implemented as an operating system for public value rather than a technology project, is offered as a design stance for practitioners.

Executive Summary

Digital Public Infrastructure succeeds when foundational digital systems become trusted, usable and sustainable public infrastructure. The challenge is therefore not simply how to build a platform. It is how to move from strategy to safe scale while maintaining interoperability, security, privacy, inclusion, accountability and long-term adoption.

The Universal DPI Safeguards Framework defines five lifecycle stages: Conception and Scoping, Strategy and Design, Development, Deployment, and Operations and Maintenance. It also identifies five implementation pathways covering legal and regulatory, institutional structures, technical foundations, capacity and resources, and a whole-of-society approach. (DPI Safeguards Initiative, 2026a).

This paper proposes a complementary DPI Scale-to-Value Framework connecting strategic intent, technical architecture, data governance, AI adoption and organisational change.

Core proposition: DPI should be implemented as an operating system for public value, not as a technology project.

Architecture, governance, adoption and safeguards should therefore be designed as one system.

The execution cycle is: Align → Architect → Govern → Build → Pilot → Scale → Learn. Each stage produces evidence for the next.

1. The Implementation Gap

Digital transformation programmes often fragment execution. Policy teams define objectives, technology teams design platforms, data teams establish standards, procurement selects suppliers and change teams manage adoption, without a single operating architecture connecting them.

DPI magnifies this problem because foundational components are reused across services and institutions. A weakness in identity, payments, data exchange, authentication or governance can propagate across an ecosystem.

The DPI Safeguards Initiative describes safeguards as active operational practices and emphasizes country-level execution, local capacity, multistakeholder coalitions and practical safeguard measures. (DPI Safeguards Initiative, 2026a).

Implementation principle: The unit of transformation is not the platform. It is the ecosystem of people, institutions, technology, data, processes and incentives that must operate together.

2. The DPI Scale-to-Value Framework

Stage	Primary question	Decision gate
Align	What public value, problem and population need are we solving?	Purpose and mandate approved
Architect	What technical, institutional and service architecture is required?	Target architecture approved
Govern	Who controls data, risk, standards, procurement and accountability?	Governance model approved
Build	Can the system be built securely, interoperably and maintainably?	Release readiness confirmed
Pilot	Does it work in real-world conditions for real users?	Evidence-based scale decision
Scale	Can it expand without reducing safety or service quality?	Controlled scale approval
Learn	What does evidence tell us to change?	Improvement cycle begins

3. Strategic Alignment

A DPI programme should begin with a theory of public value. Strategy should define the problem, target populations, service outcomes, institutional mandate, legal basis, success measures and constraints.

- Define the public problem before selecting technology.
- Identify beneficiaries and people who may be excluded.
- Establish measurable service and societal outcomes.
- Map dependencies on law, institutions, funding and existing infrastructure.
- Define what must remain public, private, interoperable or contestable.
- Define a minimum viable foundation rather than attempting to digitise everything simultaneously.

A useful strategic test is: Would the programme still make sense if the technology changed? If not, the strategy may be technology-led rather than outcome-led.

4. Technical Architecture

Domain	Design principle
Identity	Secure, privacy-aware identity and authentication with recovery and redress.

Payments	Interoperable interfaces and resilient transaction processing.
Data exchange	Standards-based APIs, controlled sharing and purpose-limited access.
Security	Security-by-design, least privilege, monitoring, incident response and resilience testing.
Interoperability	Open standards and modular interfaces to reduce lock-in.
Observability	Operational telemetry without unnecessary surveillance.
Resilience	Failure, recovery, degraded operation and continuity by design.
Portability	Data, interfaces and operational knowledge can transition where appropriate.
Local maintainability	Local engineering capability and documentation are part of the operating model.

5. Architecture Decision Records

Major architectural choices should be captured in short, reviewable Architecture Decision Records covering the decision, alternatives, assumptions, risks, interoperability, security/privacy, cost, owner and review date. This creates institutional memory and reduces dependence on individual staff or suppliers.

6. Data Governance

Data is the connective tissue of DPI. Weak data governance can undermine privacy, security, service quality, interoperability and trust even when the technology is technically sound.

Control	**Implementation requirement**
Purpose	Document why data is collected, used and shared.
Ownership	Assign accountable data owners and operational stewards.
Classification	Classify information according to sensitivity and consequence.
Access	Apply least privilege and appropriate role/attribute controls.
Quality	Define accuracy, completeness, timeliness and correction mechanisms.
Privacy	Embed minimisation, purpose limitation, retention and data-subject protections.
Security	Protect data at rest, in transit and during authorised use.
Interoperability	Use common data models, standards and APIs where appropriate.
Provenance	Maintain traceability of material data sources and transformations.
Retention	Define lifecycle rules rather than indefinite retention.
Redress	Enable correction and appropriate challenge where data affects people.

Audit	Maintain evidence of material access, use, changes and disclosures.

7. AI Adoption as a Managed Capability

AI should be introduced progressively into DPI rather than treated as a single technology deployment. The governance burden should increase with consequence, autonomy, scale and interconnectedness.

Level	**Illustrative use**	**Governance emphasis**
Assist	Search, summarisation, translation, knowledge support	Human review, disclosure and data controls
Recommend	Risk scoring, prioritisation, decision support	Validation, bias testing and accountable decision owner
Automate	Routine actions within defined boundaries	Rules, monitoring, exception handling and intervention
Act	AI initiates or executes consequential actions	Strict authorisation, human oversight, testing and rollback
Coordinate	Multiple agents or systems collaborate across workflows	System-level controls, identity, permissions, observability and containment

AI adoption gates: Use-case justification → Data readiness → Risk classification → Human oversight → Technical assurance → Pilot evidence → Scale approval.

8. Operating Model and Change

Technology adoption is an organisational transformation problem. DPI programmes require institutional ownership, multidisciplinary capability, incentives, communications, training and feedback loops.

Capability	**Implementation action**
Leadership	Create a cross-functional accountable steering structure.
Product ownership	Assign owners responsible for outcomes, not only delivery.
Technical capability	Build local architecture, engineering, cybersecurity, data and AI capability.
Operations	Define service, incident, continuity and maintenance responsibilities.
Change management	Map affected roles, incentives, behaviours and training needs.
User adoption	Measure onboarding, completion, repeat use, trust and drop-off.
Community engagement	Create structured feedback mechanisms for affected communities.

Knowledge transfer	Require documentation and capability transfer from external suppliers.

9. Procurement as an Implementation Lever

- Open standards and interoperability requirements.
- Clear data ownership, access, portability and deletion obligations.
- Security, privacy and incident-response requirements.
- Architecture and API documentation plus audit rights.
- Business continuity and disaster recovery.
- Subcontractor transparency and material-change controls.
- Knowledge transfer and local capability development.
- Exit, transition and vendor-lock-in mitigation.

Procurement test: Can the institution still govern and evolve the service if the supplier, product or underlying technology changes?

10. Pilot-to-Scale Evidence

A pilot is evidence generation, not merely a smaller version of national scale. It should deliberately test assumptions most likely to fail during expansion.

Dimension	**Pilot question**
Technical	Does the system perform under realistic load and failure conditions?
User	Can intended users complete the journey successfully and safely?
Inclusion	Who is unable or less likely to use the service, and why?
Security	What vulnerabilities or attack paths emerge in real conditions?
Privacy	Are data flows consistent with intended purpose and controls?
Institutional	Can responsible authorities operate without exceptional support?
Economic	Are lifecycle costs and financing assumptions credible?
Trust	Do users understand, trust and accept the service?
AI performance	Does AI perform consistently across relevant contexts and groups?
Safeguards	Are complaint, intervention, audit and redress mechanisms operational?

11. Scale Readiness Scorecard

Dimension	Readiness question
Strategy	Is public value validated?
Architecture	Is the architecture resilient, interoperable and maintainable?
Data	Are governance, quality, privacy and security controls operational?
AI	Are use-case boundaries, oversight and monitoring tested?
Institution	Are responsible authorities capable of operating the system?
People	Are users and affected groups prepared and able to participate?
Security	Are critical threats tested and incident mechanisms proven?
Redress	Can people obtain meaningful correction, appeal or human review?
Procurement	Can the programme evolve without excessive supplier dependency?
Sustainability	Is the long-term financial, institutional, technical and environmental model credible?

12. Implementation Dashboard

Outcome	Example metric
Adoption	Activation, completion and repeat-use rates by relevant groups
Inclusion	Completion and failure rates across priority populations
Trust	User-reported confidence and understanding
Reliability	Availability, transaction failure and recovery metrics
Security	Material incidents, detection time and resolution time
Privacy	Material privacy incidents and control compliance
Data quality	Accuracy, completeness and correction rates
AI assurance	High-impact AI systems with documented testing and oversight
Redress	Complaint volume, resolution time and successful correction/appeal
Interoperability	Share of critical interfaces using approved standards
Local capacity	Critical roles with local capability and succession

Sustainability	Lifecycle cost, financing coverage and environmental measures

13. Failure Modes and Red-Team Questions

- What happens if the primary supplier exits?
- What happens if identity, payment or data exchange becomes unavailable?
- Which groups are least likely to benefit, and why?
- Can a person obtain meaningful redress without technical expertise?
- Who can stop the system when a serious safeguard failure occurs?
- Which data flows would create the greatest harm if misused?
- What happens when an AI model performs poorly for a minority population or new context?
- Which assumptions are being treated as facts rather than tested evidence?
- Does the operating model remain viable after initial programme funding ends?
- Can the institution explain and defend the architecture five years after the original team has left?

These questions convert implementation from a delivery exercise into a resilience and accountability exercise.

14. Alignment with the DPI Safeguards Framework

This framework deliberately complements rather than reproduces the Universal DPI Safeguards Framework. Its five implementation layers connect to the Initiative's five pathways.

DPI pathway	**This framework's contribution**
Legal & Regulatory	Mandates, data governance, procurement and redress requirements
Institutional Structures	Operating model, accountable owners, assurance and escalation
Technical Foundations	Architecture, interoperability, security, privacy and AI controls
Capacity & Resources	Local capability, training, financing and knowledge transfer
Whole-of-Society	Adoption, participation, inclusion, feedback and trust measurement

The alignment is deliberate because the current DPI Safeguards resources provide adoption pathways, assessment resources and measurable outcomes/indicators intended to help Responsible Authorities identify gaps and operationalise safeguards. (DPI Safeguards Initiative, 2026b, 2026c).

15. Worked Example (illustrative)

Consider a hypothetical country building a national digital identity and payments foundation. In Align, the programme defines its public value as universal benefit access and documents the legal mandate and success measures; the gate is an approved purpose and mandate. In Architect, the target design chooses open standards, layered APIs and a privacy-aware identity model, with major choices recorded in Architecture Decision Records; the gate is approved target architecture. In Govern, a data governance body assigns ownership, classification and redress rules before any large-scale integration; the gate is an approved governance model. In Build, the release candidate passes security, interoperability and recovery testing. In Pilot, two regions deliberately test failure and exclusion: low-connectivity users, agent-assisted channels, downtime behaviour; the gate is an evidence-based scale decision, not a launch date. In Scale, expansion proceeds in controlled waves, with the scorecard demanding fresh evidence that safety and service quality hold at each wave, because scale is treated as a new risk state. In Learn, dashboard evidence on adoption, trust, inclusion and incidents feeds back into architecture and policy. This example is hypothetical and illustrates the framework; it reports no real programme.

16. Strategic Recommendations

1. Start with public value and user need, not technology selection.
2. Treat technical, institutional and governance architecture as one design problem.
3. Make interoperability and portability explicit requirements from the beginning.
4. Establish data governance before large-scale data integration.
5. Adopt AI progressively through evidence-based gates.
6. Make procurement a strategic safeguard and architecture lever.
7. Pilot for failure and exclusion, not only technical success.
8. Build local capability and knowledge transfer into programme economics.
9. Measure adoption, trust, inclusion, safety and resilience alongside technical KPIs.
10. Treat scale as a new risk state requiring fresh evidence.

Conclusion

DPI is infrastructure. Infrastructure succeeds when it is reliable enough to trust, flexible enough to evolve, inclusive enough to serve people with different capabilities and circumstances, and governable enough to remain accountable.

The implementation challenge is broader than technology delivery. It is the coordination of strategy, architecture, data, AI, institutions, people, procurement, safeguards and evidence.

The central shift proposed by this paper is from “build and deploy” to “align, architect, govern, build, pilot, scale and learn.”

The measure of successful digital transformation is not the number of systems launched. It is the durable public value created, the people included, the risks controlled and the institutional capability left behind.

Limitations

The Scale-to-Value Framework, its decision gates, AI adoption levels, scorecard and dashboard are independent practitioner proposals. They have not been tested in a live DPI programme, and no empirical validation is claimed. The framework aligns with the Universal DPI Safeguards Framework's lifecycle stages and implementation pathways but is not an official adoption tool of the DPI Safeguards Initiative, and alignment implies no endorsement. Dashboard metrics are illustrative and must be adapted to institutional context. Sources were reviewed in August 2026 and continue to evolve. The author writes as an independent practitioner; the framework reflects implementation experience and public materials rather than primary field research.

References

DPI Safeguards Initiative (2026a) Universal DPI Safeguards Framework, Version 2.0. Available at: https://www.dpi-safeguards.org/framework (Accessed: 16 August 2026).

DPI Safeguards Initiative (2026b) DPI Safeguards Assessment and Adoption Pathways (resource collection). Available at: https://www.dpi-safeguards.org/assessments (Accessed: 16 August 2026).

DPI Safeguards Initiative (2026c) Resources: Guide, Adoption Pathways and Assessment. Available at: https://www.dpi-safeguards.org/resources (Accessed: 16 August 2026).

Author's Note

This working paper is an independent practitioner contribution. It is not an official publication of the United Nations, UNDP, the DPI Safeguards

Initiative or any other international organization. It does not claim endorsement, authorship or institutional affiliation with the official Universal DPI Safeguards Framework. The Scale-to-Value Framework, decision gates, AI adoption controls, scorecard and dashboard are

proposed practitioner contributions.

Audit note

Reviewed against current public DPI Safeguards materials available on 16 August 2026. The paper deliberately uses the official framework's lifecycle and pathways as alignment points while presenting its implementation architecture as an independent contribution.