Digital Public Infrastructure for Governments: Evidence and Risks

Read online with charts and updates:
https://risalatconsultants.com/digital-public-infrastructure-governments-evidence-risks/

Key Takeaways

Digital public infrastructure can make government faster and more inclusive, but only when agencies change how they work and protect the data they hold.

- Shared building blocks - digital public infrastructure means identity, payments and data exchange that many services share.
- Measured results exist - the World Bank reports benefit processing in the Philippines cut from four days to one and 8 million new bank accounts linked to its programme.
- New investment - Nepal's US$50 million Digital Transformation Project, approved in February 2026, finances a data exchange, digital credentials, cybersecurity and data governance.
- Security lags behind - ITU found that capacity development and technical measures are the weakest areas of cybersecurity in most countries.
- Design matters - privacy by design, clear ownership and offline alternatives decide whether DPI earns public trust.

Introduction

Digital public infrastructure for governments means shared digital systems, such as a national digital identity, interoperable payments and a secure way for agencies to exchange data, that many public and private services can build on. Instead of every ministry creating its own database and verification process, services draw on common building blocks, which can cut processing times, reduce duplication and make it easier for people to access services and finance.

The idea is now at the centre of many government reform programmes and development partner portfolios. The evidence shows real gains where it is done well, but also real risks: cyber attacks, misuse of personal data, fraud and exclusion of people who cannot use digital channels. This article sets out what the evidence says, what can go wrong, and what governments can do to get it right.

What Digital Public Infrastructure Includes

Most definitions group digital public infrastructure into three foundations:

- Digital identity: a trusted way for people to prove who they are online and offline
- Digital payments: interoperable systems for government transfers and everyday payments
- Data exchange: secure, rule-based sharing of data between agencies, with consent where required

On top of these, governments build services: citizen portals, social registries, digital credentials, electronic signatures and e-procurement. Nepal's Digital Transformation Project illustrates the full stack. The World Bank approved US$50 million on 9 February 2026 to finance an integrated online citizen service portal, an integrated social registry, a secure government-wide data exchange and a digital locker for verifiable credentials, along with electronic signatures,

cybersecurity and data governance. ADB is to contribute a further US$40 million as co-financier, and the implementing agencies include the Ministry of Communications and Information Technology and the Department of National ID and Civil Registration.

The Evidence: Efficiency, Inclusion and Revenue

Government efficiency

The World Bank's Global Digital Public Infrastructure Program reported in May 2026 that in the Philippines benefit processing was cut from four days to one and business permit processing was reduced by 80 percent. These gains came from combining digital identity with redesigned processes, not from technology alone.

Identity and financial inclusion

The same World Bank results report that 80 million people are enrolled in the Philippines' national ID system, PhilSys, with 60 million IDs issued and 8 million new bank accounts opened. In Nigeria, over 100 million National Identity Numbers have been issued, and a social protection programme supported by the World Bank reaches over 8 million households. These figures show the scale DPI can reach; they do not prove that every account or payment exists only because of the ID system.

Tax and public finance

Revenue administration is another area of investment. In Bangladesh, the World Bank's SITA project, approved in June 2025 with US$250 million, supports five agencies including the National Board of Revenue and the procurement authority, whose second-generation e-GP it will develop. Such projects create the conditions for better compliance and transparency, but revenue gains depend on administration, legal safeguards and measurement, and should not be assumed.

The Risks: Cybersecurity, Privacy, Fraud and Exclusion

Cybersecurity capacity

The importance of cybersecurity for government agencies grows with every service moved online. ITU's Global Cybersecurity Index 2024 found that legal measures are the strongest cybersecurity pillar for most countries, while capacity development and technical measures are relatively weak. It also reported progress: 139 countries had active computer incident response teams, up from 109, and 132 had a national cybersecurity strategy, up from 107. Laws and strategies are spreading faster than the skills and technical controls needed to apply them.

Privacy and misuse of data

Shared identity and data exchange concentrate personal data. Without clear purpose limits, access controls and oversight, data collected for one service can be used for another without people's knowledge, which erodes trust and may break the law.

Fraud and operational risk

Common risk categories include account takeover, impersonation, unauthorised access to registries, mistakes in identity matching, payment reconciliation failures and outages. Each needs an owner, controls and a response plan.

Exclusion

People without devices, connectivity, documents or digital skills can be left out when services become digital only. Assisted channels and offline alternatives must be designed in from the start.

Privacy by Design: What Governments Can Do

Privacy by design means building data protection into systems, rules and services before launch, rather than fixing problems after they appear. In practice, governments can:

- Collect only the data each service needs and state its purpose
- Carry out a privacy impact assessment before launching or connecting systems
- Define who owns each dataset and who may access it
- Use strong authentication, encryption and complete audit trails
- Set retention periods and delete data that is no longer needed
- Put data-sharing agreements in writing between agencies
- Test incident response and recovery before going live
- Provide a complaint route and an independent oversight body
- Keep assisted and offline channels for people who need them

Why Public Sector Technology Adoption Stalls

Many digital projects deliver systems that agencies then under-use. The usual barriers are institutional rather than technical:

- Shared platforms cross the mandates and budgets of several ministries, so no one owns the result
- Staff lack skills in service design, data management, privacy and cybersecurity
- Old paper processes continue alongside new systems
- Operating costs for hosting, licences, staff and security are not budgeted after the project ends
- Success is measured by systems delivered, not by services used

What works is the opposite: a lead institution with a clear mandate, written agreements between agencies, staff training before launch, measurement of real transactions and user satisfaction, and a budget for running costs.

A Practical Roadmap for Ministries and Project Units

Governments starting or scaling digital public infrastructure can follow a sequence that keeps technology, rules and people moving together:

- Agree the governance first. Designate the lead institution, set up a steering group of participating agencies and agree decision rights.
- Map the services and data. List the services that will use shared identity, payments or data exchange, the data each needs and the legal basis for using it.
- Set standards. Adopt interoperability, security and data quality standards that every agency must meet before connecting.
- Assess privacy and security risks. Carry out privacy impact assessments and security risk assessments for each new connection.
- Redesign the processes. Remove steps that the new system makes unnecessary, such as repeated document checks.
- Prepare the people. Train staff in the new processes, data handling and incident reporting

before launch, and plan support for users.
- Pilot with real users. Test with representative users, including people who need assisted channels, and fix problems before scaling.
- Measure and publish results. Report transaction volumes, processing times, failures and complaints, and use them to improve.
- Budget for operation. Plan recurring costs for hosting, licences, security monitoring, audits and specialist staff.

What to Ask Technology Suppliers and Partners

Much of the infrastructure is built or operated with suppliers and development partners. Procurement and contract teams can protect the government's position by asking clear questions before signing:

- Which open standards does the solution use, and can another supplier take over later?
- Who owns the data, the source code configuration and the documentation?
- Where is data stored, and how is it protected and backed up?
- How are security incidents detected, reported and resolved, and within what times?
- What are the full running costs over five years, including licences and support?
- How will government staff be trained to operate and supervise the system?
- How is access for people with low digital skills or disabilities ensured?

Writing the answers into contracts and service level agreements avoids lock-in and keeps control of public data with the state. It also gives auditors and oversight bodies a clear basis for reviewing the arrangement later.

Lessons From Nepal's Project Design

Nepal's Digital Transformation Project brings several of these elements into one investment: a citizen service portal and social registry for service delivery, a secure government-wide data exchange and digital credentials as shared foundations, and electronic signatures, cybersecurity and data governance as enabling rules. It also digitises high-impact services such as land administration.

For implementing agencies, the design highlights three practical tasks. First, data exchange requires written agreements on what each agency shares, under which conditions and with what safeguards. Second, digital credentials and electronic signatures require legal recognition and trusted processes so that agencies accept them in place of paper. Third, cybersecurity and data governance must be staffed and funded inside each participating agency, not only at the central level. Projects in other countries face the same tasks.

Critical Questions Government and Project Leaders Should Be Asking

Who owns each shared platform?

Name the lead institution for identity, payments and data exchange, and set out in writing what each participating agency must do.

Have we assessed privacy before connecting systems?

A privacy impact assessment for each new data flow is cheaper than repairing trust after misuse.

Do we have the cybersecurity skills to run what we are building?

Check whether incident response, monitoring and secure operations are staffed, not only whether a strategy exists.

How will people without digital access be served?

Plan assisted channels, offline options and appeal routes before services become digital by default.

Are we measuring use, not just delivery?

Track completed transactions, processing times, failures and complaints for each service.

Who pays for operation after the project?

Budget recurring costs for hosting, licences, security and specialist staff from the start.

How Risalat Can Help

Risalat supports ministries and project units on digital government, data governance and cybersecurity through its digital government programmes. Agencies can test their starting point with the free digital readiness assessment and the cybersecurity basics assessment.

Frequently Asked Questions

What is digital public infrastructure?

Shared digital building blocks such as digital identity, payment systems and secure data exchange that many public and private services can use, instead of each agency building its own.

Does digital public infrastructure improve government services?

It can. The World Bank reports that in the Philippines benefit processing was cut from four days to one and business permit processing was reduced by 80 percent, but results depend on how agencies change their processes, not only on the technology.

Why is cybersecurity important for government agencies?

Government systems hold sensitive personal data and run essential services, so an attack can stop services, expose citizens and damage trust. ITU's Global Cybersecurity Index 2024 found that capacity development and technical measures are relatively weak in most countries.

What does privacy by design mean for government DPI?

Building data protection into the system from the start: collecting only necessary data, limiting its use to the stated purpose, controlling access, keeping audit trails and assessing privacy risks before launch.

Sources

- World Bank: Global Digital Public Infrastructure Program, From Foundations to Scale (May 2026)
- World Bank: Nepal, World Bank approves US$50 million Digital Transformation Project (9 February 2026)
- ITU: Global Cybersecurity Index 2024, press release
- World Bank: SITA project, Bangladesh (June 2025)

Related Risalat programmes

- Digital Government, Public Sector Innovation & Service Delivery Excellence Training, Tallinn (1 Feb 2027)
- Cybersecurity Fundamentals for Business Leaders, Singapore (26 Jan 2027)
- Training Course on Cybersecurity in Digital Health in Tallinn, Tallinn (8 Feb 2027)

Talk to us about your institution or project: https://risalatconsultants.com/reach-risalat/