



INTERNATIONAL RESEARCH INSTITUTE — SECTOR REPORT

Digital Government and the Future of Public Service Delivery

Public sector technology · 2026-09-03 · Licence CC BY 4.0

The shift in brief

For most of the past two decades, "digital government" meant putting a form online. A citizen who had once queued at a counter could download a document, book an appointment or file a return through a website. This was a real convenience but a thin one: the digital layer sat on top of unchanged institutions, and the hard parts of public administration — verifying who someone is, moving money to them, and letting one agency safely reach data held by another — remained manual, siloed and slow. The defining shift of the current period is that governments have begun to build those hard parts as shared, reusable infrastructure rather than as features of individual websites. Digital identity, government-to-person payment rails and interoperable data-exchange layers are increasingly treated as public plumbing on which many services run — a model now widely described as digital public infrastructure.

This report treats that shift — from services-as-websites to services-as-infrastructure — as the central analytical fact of the market. It changes what governments buy, how value is created, and where the risks lie. The country cases that have moved fastest, from Estonia's data-exchange layer to India's identity and payment stack to Ukraine's crisis-accelerated services app, are distinguished less by the sophistication of their front-end design than by having built trusted foundational layers and the institutional arrangements — legal mandates, data-protection rules, procurement capability — that let many services reuse them. Where those foundations are absent, additional spending on portals yields diminishing returns.

Two forces will shape the market to 2032. The first is a persistent gap between the largest line of spending and the largest source of visible value. Most public digital budgets are consumed not by citizen-facing applications but by the unglamorous modernisation of core back-office systems — decades-old case-management, tax, benefits and registry platforms — and by migrating them to cloud. Legacy debt and a long record of large-project failure make this the binding constraint on delivery. The second is the rise of identity as the pivotal layer: it is at once the greatest enabler of joined-up, proactive services and the greatest source of exclusion, surveillance and concentration risk, which is why its governance is becoming the central policy question.

Our central judgement is that digital government is a durable, structurally growing market, but one where value is gated by institutions rather than technology. We estimate the broad addressable market at roughly USD 400–600 billion in 2025 and sketch a 2032 range of about USD 700 billion to USD 1.2 trillion under explicitly stated assumptions. The wide band reflects genuine uncertainty about definitional boundaries, the pace of legacy modernisation, and whether public trust in shared identity and data systems holds. Decision-makers should plan for a market that grows steadily but rewards institutional readiness — clean registries, capable procurement, credible data protection — over the purchase of any particular platform.

By the numbers

INDICATOR	VALUE
Broad addressable digital-government market, 2025 — broad definition; estimate	USD 400–600bn
Sketched 2032 range — scenario band, not a forecast	USD 700bn–1.2tn
People without official proof of identity — World Bank estimate	~850 million
Implied CAGR to 2032 — under stated assumptions	~8–11%

Principal messages

- The unit of digital government has changed from the website to the shared layer.** The frontier is no longer a well-designed portal but reusable identity, payment and data-exchange infrastructure that many services draw on. This reframes the market around foundational rails and their interoperability, and explains why some middle-income systems now move faster on population coverage than wealthier ones weighed down by fragmented legacy estates.
- Most spending is invisible to citizens.** Core-systems modernisation and cloud migration — not apps and portals — absorb the majority of public digital budgets, which we estimate at roughly USD 250–380 billion of the 2025 market. Legacy debt and a long record of large-project overruns make delivery, not technology selection, the binding constraint.

- **Identity is the pivot, for value and for risk.** Foundational digital identity most enables proactive, joined-up services and, at the same time, most concentrates risk — of exclusion for those who cannot enrol or authenticate, of surveillance and function creep, and of catastrophic single points of failure. Its governance is becoming the defining policy question of the field.
- **Regional models are diverging strategically.** The European Union is pursuing a rights-based path built on data protection, the once-only principle and a common digital identity wallet; an open, reusable model associated with India is being adopted across the global South on open-source components; and much of the rest of the world is modernising in a more fragmented, federated way. A single global template is neither emerging nor, on the evidence, desirable.
- **The market is real but institutionally gated.** Its returns depend on institutional conditions — procurement capability, data governance, workforce skills and public trust — that money alone does not buy. The systems that scale are those that treat digitalisation as institutional reform, not as an IT purchase.
- **Trust is the load-bearing asset, and public value is hard to measure.** Because these systems mediate identity, money and personal data, their value collapses if citizens do not trust them: data protection, transparency, redress and inclusive design are preconditions for adoption, not compliance overhead. Yet governments rarely evaluate digital programmes against counterfactual outcomes, so capital is often allocated on aspiration and comparison rather than evidence.

1. Context and why it matters

Public administration has always been an information-processing enterprise. Registering a birth, assessing a tax liability, paying a pension or issuing a licence is at root a matter of establishing identity, applying a rule, recording a decision and, often, moving money. The digitalisation of government is therefore not a peripheral modernisation of citizen-facing channels but a reworking of the core machinery of the state — which is why it bears directly on the fiscal efficiency of government, the reach and fairness of public services, and the relationship between citizen and state.

The first two decades of e-government focused on the front end. Governments built websites, digitised forms and stood up transactional portals, guided by the intuition that citizens should be able to deal with the state as easily as with a bank. This produced genuine gains and well-known reference points — the United Kingdom's consolidation of hundreds of departmental sites into a single platform from 2011, the spread of dedicated digital-service units, and the rise of countries such as Denmark, Estonia, the Republic of Korea and Singapore in the biennial United Nations e-government rankings. But it also revealed the limits of a front-end strategy: a well-designed form still had to reach a legacy system behind it, and a service needing data from three agencies still asked the citizen for it three times.

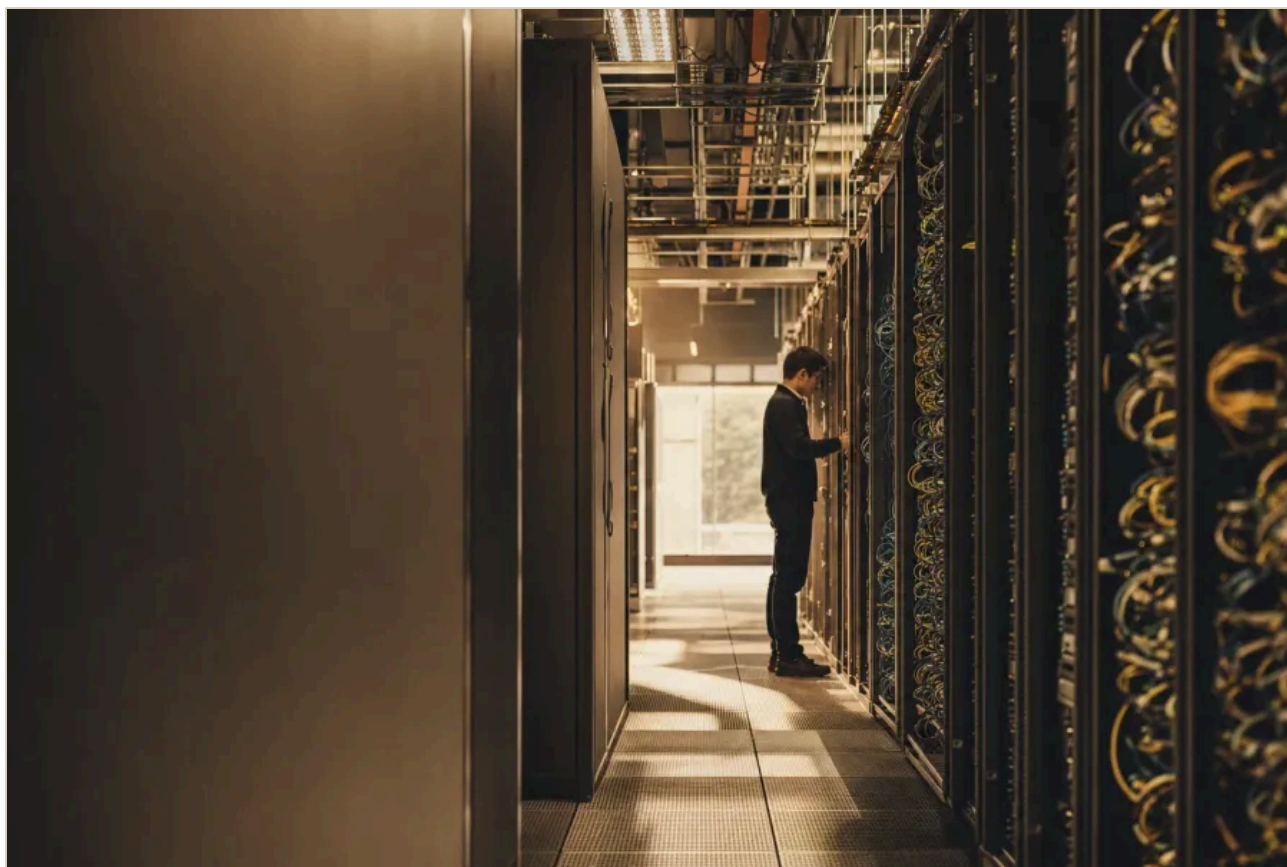
The current period is defined by the attempt to fix the back end and the connective tissue. The organising idea is digital public infrastructure: treating identity, payments and data exchange as shared, society-wide utilities — analogous to roads or the electricity grid — on which both public and private services can be built. It gained international profile during India's 2023 presidency of the Group of Twenty, which placed digital public infrastructure on the multilateral agenda and framed it as a route to faster development. The significance for decision-makers is that the questions have changed: no longer only "how good is our website?" but "do we have a trusted identity layer, can money reach people directly, can our systems talk to one another, and are the rules and institutions in place to make all of that safe?" Those are questions of institutional design as much as of technology.

2. Market structure and scale

Estimating the size of the "digital government market" is complicated by where one draws the boundary. A narrow definition counts only dedicated govtech platforms and the programmes governments describe as such. A broad definition adds the far larger sum spent modernising core information systems, migrating to cloud and securing all of it — digitalisation in substance even when it is not labelled a flagship programme. These definitions differ by a wide margin, so any single headline figure is misleading without its boundary stated; we therefore present a segmented estimate with explicit assumptions rather than a single number.

The market is best read as a set of layers with very different economics. At the foundation sit three shared rails: **digital identity and credentials**, which establish who a person is; **government-to-person payment and disbursement**, which move money to and from citizens; and **data exchange and interoperability**, which let agencies reach one another's records under rules. Above

these sit **citizen-facing service platforms and portals**, the visible front door. Underneath and around everything sits the largest cost of all — **core-systems modernisation and cloud migration**, the replacement or renewal of the ageing case-management, registry, tax and benefits systems that actually run public services — together with **cybersecurity and assurance** for government, and an emerging layer of **artificial intelligence and automation** in public administration.



Digital government read as layers: shared identity, payment and data-exchange rails; the citizen-facing platforms that sit on them; and the large, largely invisible cost of modernising and securing core back-office systems. Value concentrates in the shared rails and institutions; spending concentrates in legacy modernisation. — IRI

The estimates below are our own triangulation from official statistics on government information-technology expenditure, published national digital strategies and budgets, multilateral and development-bank programme data, and the direction and magnitude implied by recurring cross-country indices. They are transparent estimates, not measured figures, and the ranges are deliberately wide.

SEGMENT	2025 GOVERNMENT SPEND (ESTIMATE, USD)	BASIS / ASSUMPTIONS	CONCENTRATION	2025–2032 GROWTH CHARACTER
Digital identity & credentials	15–30bn	National ID, credentialing and authentication programmes; excludes wider registries	Moderate; open-source options rising	Foundational; policy-sensitive
Government-to-person payments	20–40bn	Disbursement rails, benefits and subsidy delivery, treasury digitalisation	Moderate	Steady; scaled during COVID-19
Data exchange & interoperability	10–20bn	Exchange layers, registries interconnection, once-only implementations	Fragmenting	Fast from a small base
Citizen-facing platforms & portals	40–70bn	Single portals, service platforms, digital-service units	Low, contestable	Maturing; diminishing marginal returns
Core modernisation & cloud	250–380bn	Legacy replacement, ERP, cloud migration of core systems	Moderate; large integrators	Largest line; slow, delivery-constrained
Cybersecurity & assurance	40–70bn	Government security, identity assurance, resilience	Moderate	Rising with threat and dependence
AI & automation (emerging)	10–25bn	Automation, decision support, service AI pilots	Low, early	Fastest-growing from a small base
Broad total (overlaps removed)	~400–600bn	Sum less double-counting of embedded security and cloud	—	Central 2032 range: ~700bn–1.2tn

Plotting each segment's stated low and high bounds makes the shape of the market visible. Core modernisation and cloud dominate the picture — a single band larger than all the others combined — which is precisely the point: the money is concentrated where the citizen never looks, in the renewal of systems that already exist.

2025 digital-government spend by segment — low–high estimate range

CATEGORY	LOW ESTIMATE (USD BN)	HIGH ESTIMATE (USD BN)
Identity	15	30
G2P payments	20	40
Data exchange	10	20
Portals	40	70
Core modernisation	250	380
Cybersecurity	40	70
AI & automation	10	25

Section 2 estimate ranges, shown before removing double-counting. Core modernisation and cloud dominate; the broad total (~USD 400–600bn) nets out overlapping security and cloud. Estimates, not measured values.

Two features of this structure deserve emphasis. First, the **largest spend and the largest value are in different places**: the largest line item is legacy modernisation, which is defensive and delivery-constrained, while the largest source of new value is the thin, shared layer of identity, payments and interoperability that lets many services be built once and reused. A government can spend heavily on the former and still fail to deliver joined-up services if it neglects the latter. Second, **concentration varies by layer**. Core modernisation is dominated by a few large systems integrators and cloud providers, raising lock-in and dependency questions; identity and interoperability are increasingly served by open-source, reusable components, which lowers cost but shifts the challenge onto governance and integration capability.

Worldwide government information-technology spending is widely estimated to run into the high hundreds of billions of dollars annually, so on our broad definition digital government in 2025 is a large share of a very large budget, not a niche. Its significance lies less in year-on-year growth than in composition: the shift of spending toward shared infrastructure and away from bespoke, single-agency systems. The 2032 range we sketch — roughly USD 700 billion to USD 1.2 trillion — assumes high-single-digit to low-double-digit compound annual growth, sustained legacy modernisation rather than repeated project failure, and no severe erosion of public trust. It is a scenario band, not a forecast, and Section 7 sets out the conditions under which the lower or upper bound becomes more likely.

3. Drivers: what is moving the market

Four forces are pushing governments from front-end digitisation toward infrastructure-led delivery. The first is **fiscal pressure**. Ageing populations, elevated public debt and constrained tax bases mean ministries are asked to deliver more with the same or fewer resources, and administrative efficiency is one of the few levers available. Digitalising the core — automating eligibility checks, reducing manual re-keying, cutting fraud and error in payments — offers measurable savings where delivered, which is why finance ministries, not only technology units, increasingly sponsor these programmes.

The second is **citizen expectation**. People who bank, shop and communicate through instant, well-designed digital services carry those expectations to their dealings with the state, and the gap between a two-minute private-sector transaction and a two-week government one has become politically salient across income levels. The third is the **maturation of the shared-infrastructure model** itself. A decade ago, building a national identity or payments layer meant a bespoke, high-risk megaproject; today, reusable and often open-source components — modular identity platforms and interoperability toolkits developed as international public goods — lower the cost and risk of entry, so more governments can build foundational layers without commissioning everything from scratch.

The fourth is the **demonstration effect of crisis and of visible success**. The COVID-19 period was a forcing event: governments that could identify people and move money to them digitally delivered emergency support at speed, while those that could not resorted to slow, leaky, manual disbursement. Visible national successes reinforced the lesson — Estonia's long-standing data-exchange architecture, the rapid rollout of a widely used services application in Ukraine under wartime conditions, and the scale achieved by India's identity and real-time payment systems, the latter now widely reported to process billions of transactions

each month. These examples function less as templates to copy than as proof that the infrastructure model can work at population scale, which shifts the political calculus from whether to build to how.

The forcing effect of crisis — The COVID-19 period rewarded governments that could identify people and pay them digitally, and exposed those that could not. It durably raised the political priority of foundational identity and payment rails — the shared layers on which proactive, at-scale service delivery depends.

4. Where value accrues: the identity and interoperability core

If the largest spending is in legacy modernisation, the largest new value is in the thin foundational layer — and within it, in identity above all. A trusted, inclusive digital identity is the precondition for almost everything else: for paying the right person, pre-filling a form with data the government already holds, letting a citizen prove an attribute without disclosing unrelated information, and moving from reactive services citizens must seek out to proactive ones the state can offer automatically. The governments capturing the most value are those that have built identity as a genuine public utility — inclusive, privacy-protective and reusable across sectors — rather than as a single agency's login.

Interoperability is the multiplier. The economic case for shared infrastructure rests on the "build once, reuse many times" principle: a data-exchange layer that lets agencies query one another's registries under clear rules turns each new service from a bespoke integration project into a configuration of existing components. The European Union has codified the citizen-facing version of this as the once-only principle — the expectation that people should not supply the same information to the state twice — and is building the means to deliver it across borders. The value is real but conditional: it materialises only where the legal basis for data sharing, the data-protection safeguards and the technical standards all hold together. Where any one is missing, interoperability stalls and the promised reuse does not occur.

"The largest public digital budgets are spent where the citizen never looks; the largest public value is created in the thin, shared layer they never see."

— §4, *Where value accrues*

The economics of the layers differ sharply, and this matters for procurement and competition. Core modernisation and cloud are capital-intensive, integration-heavy and dominated by a few large suppliers, creating durable dependency and lock-in that governments frequently underestimate at the point of purchase. The foundational rails, by contrast, are increasingly buildable from open, reusable components, which lowers direct cost but relocates the hard part to institutional capability — the ability to govern, integrate and maintain shared infrastructure over decades. The implication is that the return on internal capability, clean registries and enforceable data-sharing rules will typically exceed the return on any single procurement, because it is the reusable foundation, not the individual system, that compounds in value.

5. Governance, regulation and the comparative regional lens

Governance has moved to the centre of the digital-government conversation because these systems now mediate identity, money and personal data at population scale, and because trust is the asset on which their value depends. The regulatory frame is set by data-protection law, by identity and interoperability regulation, and by the emerging rules for artificial intelligence in the public sector. In the European Union, the General Data Protection Regulation established a rights-based baseline for how public bodies may process personal data; the revised electronic-identification framework adopted in 2024 goes further, requiring member states to offer citizens a common European Digital Identity Wallet and setting standards for cross-border recognition; and the once-only principle, embedded in the Single Digital Gateway, obliges administrations to reuse data they already hold rather than ask again. Together these make the European model distinctive: rights-based, interoperable by design, and willing to accept some added cost in exchange for legal certainty and fundamental-rights protection.

Alongside binding law, a layer of shared, reusable technology and reference standards is professionalising the field. Modular open-source identity platforms and interoperability toolkits, stewarded as international public goods, are lowering the cost of foundational infrastructure across the global South. Multilateral and development-bank programmes have made legal identity and digital public infrastructure explicit development objectives, reflected in the widely cited World Bank estimate that roughly 850 million people still

lack official proof of identity — a gap that is both a development problem and, handled carelessly, a source of exclusion risk. The timeline below traces how the field has moved from front-end portals toward shared, governed infrastructure.

From portals to governed public infrastructure

WHEN	MILESTONE	DETAIL
2007–2012	Front-end era and digital-service units	Governments consolidate departmental websites and stand up dedicated digital-service teams; the focus is transactional portals and better forms.
2014–2018	Foundational rails scale nationally	Large-scale digital identity and real-time payment systems reach population scale in leading cases, and data-exchange architectures mature, shifting attention to shared infrastructure.
2020–2021	Pandemic forcing event	Government-to-person payments and digital identity prove decisive for emergency support, durably raising the priority of foundational layers.
2023	Digital public infrastructure goes multilateral	Digital public infrastructure is placed on the Group of Twenty agenda, framing shared identity, payments and data exchange as a development strategy.
2024	Rights-based identity regulation	The European Union's revised electronic-identification framework requires member states to offer a common Digital Identity Wallet, setting a rights-based reference model.
2025 onward	AI and assurance obligations	Rules for artificial intelligence in the public sector and rising assurance requirements begin to shape how automated decisions may be used in service delivery.

The regional picture is genuinely divergent, and the divergence is strategic rather than merely a matter of pace. The **European Union** leads with comprehensive, rights-based, interoperable regulation and a common identity wallet, prioritising legal certainty and fundamental rights. An **open digital-public-infrastructure model associated with India** — foundational identity, real-time payments and consent-based data sharing, increasingly built on open-source components — is being adopted across South and Southeast Asia, Africa and Latin America, often with multilateral support, and can move quickly on population coverage. The **United States** modernises in a more federated, sectoral way, with capable digital-service units at federal level but authority dispersed across agencies and states. **Estonia and the Nordics** remain mature references built on early identity and data-exchange investments; **Gulf states** are investing heavily in consolidated national platforms; and many **Sub-Saharan African** systems are building identity and payments mobile-first, from a lower base and with the largest identity gaps to close. The practical lesson is that infrastructure choices are also governance choices: what is technically possible is constrained by what the legal and institutional framework will safely permit.

6. Risks and where value is destroyed

The digital-government market carries a distinctive risk profile because failure is not only commercial but civic. The most consequential risk is **digital exclusion**. Systems built around digital identity and online channels can leave behind those who lack connectivity, devices, documentation or digital confidence, or whose biometrics do not reliably enrol or authenticate. Where a digital route becomes the only practical route, exclusion shifts from inconvenience to denial of entitlement — so inclusive design, assured offline and assisted channels, and attention to authentication-failure rates are conditions of legitimacy, not optional refinements.

A second cluster concerns **privacy, surveillance and function creep**. Foundational identity and interconnected registries make the state far more capable of seeing its citizens, and systems introduced for one purpose are readily extended to others. Without strong data protection, purpose limitation, independent oversight and transparency, the same infrastructure that enables proactive

services can enable disproportionate monitoring — a risk that varies with the quality of a country's institutions and that materially shapes public trust. **Cybersecurity and concentration risk** compound this: centralising identity, payments and data creates high-value targets and single points of failure, so an outage or breach in a shared layer can cascade across many services at once.

Two further risks are institutional rather than technical. **Procurement and delivery failure** is the most reliable destroyer of value in this field: large public technology programmes have a long, well-documented record of overruns, cancellations and disappointing outcomes, driven by weak client-side capability, over-specification and lock-in to a few suppliers. And **trust and legitimacy** are load-bearing throughout — where citizens do not trust that a system is fair, secure and rights-respecting, adoption stalls regardless of technical quality, and hard-won trust is far easier to lose than to rebuild. Underlying all of these is a measurement problem: governments rarely evaluate digital programmes against credible counterfactuals, so capital is often allocated on comparison and aspiration rather than evidence.

7. Three scenarios to 2032

We present three scenarios rather than a single forecast, because the principal uncertainties — the pace and success of legacy modernisation, the durability of public trust in shared identity and data systems, and the degree of interoperability actually achieved — are genuinely unresolved. Each scenario is internally consistent and tied to observable signposts.

Scenarios and outlook to 2032 (broad-definition market)

A — Fragmented modernisation — Downside

Legacy modernisation continues to stall on procurement failure and lock-in; foundational rails are built inconsistently and interoperability is patchy; trust incidents in some jurisdictions slow adoption. Spending rises but value lags, and outcomes diverge sharply between leaders and laggards.

METRIC	VALUE
Market 2032	USD 700–800bn

B — Platform consolidation — Central case

The digital-public-infrastructure model mainstreams: most governments build or adopt reusable identity, payment and data-exchange layers, legacy modernisation proceeds unevenly but without systemic failure, and governance settles into a workable if costly steady state. Steady growth without a discontinuity.

METRIC	VALUE
Market 2032	USD 850bn–1.0tn

C — Interoperable public value — Upside

Shared rails, strong data protection and genuine interoperability combine to deliver proactive, joined-up services at scale; measured efficiency and inclusion gains become credible, sustaining investment and public trust across a broad base of countries.

METRIC	VALUE
Market 2032	USD 1.0–1.2tn or above

Scenario B — Platform consolidation (central case). In the most likely path, the shared-infrastructure model becomes mainstream. Most governments build or adopt reusable identity, payment and data-exchange layers; legacy modernisation proceeds unevenly, with the usual quota of troubled projects but no systemic breakdown; and governance settles into a workable, if costly, steady state anchored by data protection and identity regulation. Value arrives with a lag, concentrated among governments that pair infrastructure with institutional capability, and the market lands toward the middle of our 2032 range (broadly USD 850 billion to USD 1.0 trillion). Signposts: rising reuse of shared components, gradual improvement in project delivery, and stable public trust.

Scenario A — Fragmented modernisation (downside). Legacy modernisation continues to stall on procurement failure, lock-in and weak client-side capability; foundational rails are built inconsistently and interoperability remains patchy; and one or more high-profile trust incidents — a major breach, an exclusion scandal, or evident function creep — slow adoption in affected jurisdictions. Spending still rises relative to 2025, but value lags and outcomes diverge sharply between leaders and laggards, leaving the market near the lower bound (USD 700–800 billion). This is not a repudiation of digital government but a failure to convert spending into delivery. Signposts: continued large-project failures, stalled interoperability, and retrenchment after trust incidents.

Scenario C — Interoperable public value (upside). Shared rails, credible data protection and genuine cross-agency and cross-border interoperability combine to deliver proactive, joined-up services at scale. Measured efficiency and inclusion gains become credible, sustaining investment and public trust across a broad base of countries, and the reuse dividend compounds as each new service becomes cheaper to build, pulling spending toward the upper bound (USD 1.0–1.2 trillion or above). This requires progress on the institutional bottleneck — capability, governance and trust — not merely on technology. Signposts: credible evaluations showing realised value, rapid reuse of foundational layers, and durable public confidence.

2032 market by scenario — midpoint of stated band

PERIOD	VALUE (USD BN)
Fragmented (A)	750
Consolidation (B)	925
Interoperable (C)	1100

Midpoints of the scenario bands stated in §7 (Fragmented ~USD 750bn; Consolidation ~USD 925bn; Interoperable ~USD 1,100bn). Scenario band, not a forecast.

Across all three, our central judgement holds: the market is durable and structurally growing, but value is gated by institutions rather than technology. The scenarios differ mainly in the success of legacy modernisation, the strength of governance and trust, and the degree of interoperability achieved — not in the direction of travel.

8. Implications across the field

For governments and policymakers

Treat digitalisation as institutional reform, not as an information-technology purchase. The evidence is consistent that value accrues to governments that build capability, clean their registries, and put enforceable data-sharing and data-protection rules in place — not to those that buy the most sophisticated platform. Three priorities follow. First, **invest in the foundational layer and in reuse**: a trusted, inclusive identity system, reliable payment rails and a governed data-exchange layer compound in value in a way that bespoke, single-agency systems do not. Second, **build governance in from the start** — data protection, purpose limitation, independent oversight, redress and inclusive design are preconditions for the trust on which adoption depends. Third, **rebuild client-side capability and reform procurement** to reduce lock-in and the well-documented risk of large-project failure, favouring modular, open and reusable components over monolithic, single-supplier contracts.

For international organisations and donors

The largest marginal gains lie in the systems with the widest identity and infrastructure gaps, where roughly 850 million people still lack official proof of identity. Support should prioritise inclusive, privacy-protective foundational infrastructure and the institutional capacity to govern it, using open and reusable components to avoid new dependencies. The risk to guard against is exporting infrastructure faster than the governance to make it safe: identity and data systems built without strong rights protection can entrench exclusion and surveillance. Conditioning support on data-protection frameworks, inclusion safeguards and independent oversight is therefore part of development, not an obstacle to it.

For business, suppliers and investors

Distinguish carefully between the layers of the market, which carry very different economics and risk. Core modernisation and cloud hold the largest spend but also the greatest exposure to lock-in scrutiny, procurement reform and delivery risk; the foundational and interoperability layers are smaller but structurally growing and increasingly built on open components, which rewards suppliers who can integrate and assure rather than merely license. Prefer models that demonstrate realised public value and reduce, rather than deepen, government dependency, and stress-test exposure to a Scenario A environment of stalled modernisation and trust incidents. In this market, credibility, security and evidence of outcomes will matter more than the pace of sales.

Methods, sources and caveats

This report is a synthesis, not a primary data collection. Its purpose is to integrate widely-established facts with transparent estimates and clearly labelled scenarios, and to separate the two throughout.

Approach. We combined four kinds of source material: **official statistics and budgets** on government information-technology and digital expenditure, used to gauge the magnitude of spending and to anchor digital government as a share of larger, better-measured aggregates; **government and multilateral strategy documents** — national digital strategies and development-bank and international-organisation programmes on identity and digital public infrastructure — used for the shape and direction of the market rather than precise point estimates; **regulatory and standards texts** — data-protection law, the European Union's revised electronic-identification framework and Single Digital Gateway provisions, and reference architectures for identity and interoperability — read directly to characterise the governance trajectory; and **recurring cross-country indices** on e-government maturity, used for relative position and direction, not as measures of realised value.

What is established versus estimated. Established facts used here include the existence and broad character of the systems and rules named — national digital-service units, large-scale identity and real-time payment systems, data-exchange architectures, the once-only principle, the revised electronic-identification framework requiring digital identity wallets, and the international profile of digital public infrastructure — together with the widely cited World Bank estimate that roughly 850 million people lack official proof of identity. By contrast, **every market-sizing figure and every 2032 number in this report is an estimate**, produced by triangulation and presented as a range with its assumptions stated. The segment-by-segment 2025 estimates and the 2032 scenario band in Sections 2 and 7 are our own construction; they are not measured values and should not be cited as such. Adoption and coverage are described qualitatively where published figures vary substantially with definitions, sampling and timing, and averaging them would imply a false precision.

Limitations. Definitional boundaries make the market size sensitive to how much core modernisation, cloud and embedded security are counted as "digital government", which is why we present a range rather than a single number. The field moves quickly, and figures tied to budgets, programmes and regulatory milestones will date. Measurement of realised public value is genuinely weak across governments, and we have not manufactured confidence the evidence does not support. Readers should treat the scenarios as structured reasoning about plausible futures, conditioned on stated signposts, rather than as predictions.

Independence and funding. This report was produced under the Institute's standard independence policy. It was not commissioned or sponsored by any government, supplier or interested party, and the authors hold no positions that would benefit from a particular conclusion.

Selected sources and standards

The regulatory texts, reference architectures and cross-country indices below were consulted directly; government IT-expenditure statistics anchor the market-sizing ranges.

- United Nations, Department of Economic and Social Affairs (2024). *UN E-Government Survey 2024*. UN DESA, New York.
- World Bank (2024). *Identification for Development (ID4D): Global Dataset and identity-coverage estimates*. World Bank, Washington, DC.
- OECD (2024). *OECD Digital Government Index and Digital Government Policy Framework*. OECD Publishing, Paris.
- European Parliament and Council of the European Union (2024). *Regulation (EU) 2024/1183 amending the eIDAS Regulation (European Digital Identity framework)*. Official Journal of the European Union.
- European Parliament and Council of the European Union (2016; 2018). *General Data Protection Regulation (EU) 2016/679 and Single Digital Gateway Regulation (EU) 2018/1724 (once-only principle)*. Official Journal of the European

Union.

- Group of Twenty (2023). *G20 Framework for Systems of Digital Public Infrastructure*. New Delhi.
- Ministry of Electronics and Information Technology, India (2023). *India Stack: Aadhaar, the Unified Payments Interface and consent-based data sharing*. Government of India, New Delhi.
- Modular Open Source Identity Platform (MOSIP) and GovStack (2023). *Reference architectures for digital public infrastructure*. MOSIP and the GovStack initiative.
- National and departmental government information-technology expenditure statistics (2022–2025), used to anchor the market-sizing ranges.

Suggested citation

Venkataraman, P. and Berndt, L. (2026). *Digital Government and the Future of Public Service Delivery*. Flagship Report. International Research Institute, Global Governance and Technology & Society Programmes. Licensed under CC BY 4.0.