



STRATEGIC ISSUE BRIEF

Building Digital Foundations in Small Island Digital States 2.0

FROM DIGITAL PRESENCE TO DIGITAL UTILITY AND IMPACT



Acknowledgments

This strategic issue brief, *Building Digital Foundations in Small Island Digital States 2.0*, was developed by the United Nations Development Programme (UNDP) Global Centre for Technology, Innovation and Sustainable Development, Singapore. This effort is supported by the Government of Singapore's Ministry of Foreign Affairs and the Permanent Mission of the Republic of Singapore to the United Nations in New York. This ongoing support is very much appreciated and remains essential.

The brief was authored by Jayant Narayan with support from Laura Hildebrandt and Abdullah Alrebdī.

This brief benefited immensely from the strategic guidance, technical expertise, and peer review provided by colleagues across UNDP and our partner organizations. We are particularly grateful to: Bevan Agard, Sajib Azad, Bruno Lencastre, Navya Alam, Barbora Bromova, Megan Roberts, Benjamin Bertelsen, Naveen Varshan Ilavarasan, Raja Chandrasekharan, Enrique Crespo, Alexander Hradecky, Parima Suwannakarn, Xoan Garcia and Jabarry Garnes.

We would also like to acknowledge the invaluable perspectives shared by representatives from Small Island Developing States, whose real-world experiences and insights ground this brief in practical reality.

The team also thanks Renata Figueiredo for the design and layout, and Liwen Ng and Andrea Petkovic for support with outreach and communications.

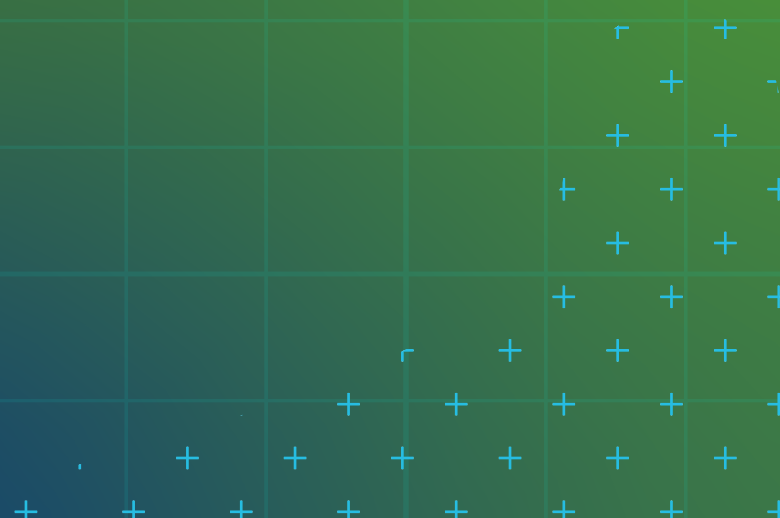
Cover photos: UNDP Pacific, Ministry of Digital Transformation Republic of Trinidad and Tobago, and Samory Araújo/PNUD-AccLab Cabo Verde

UNDP is the leading United Nations organization fighting to end the injustice of poverty, inequality, and climate change. Working with our broad network of experts and partners in 170 countries, we help nations to build integrated, lasting solutions for people and planet.

Learn more at undp.org or follow the conversation at [@UNDP](https://twitter.com/UNDP).

Copyright © UNDP 2026 All rights reserved.

The views expressed in this publication are those of the authors and do not necessarily represent those of the United Nations, including UNDP or the UN Member States.



Contents

Acknowledgments	2
-----------------	---

Executive Summary	6
-------------------	---

1. Introduction and Context	8
1.1 Latest Trends and Statistics	9
1.2 Defining Digital Foundations and Digital Utility	11
1.3 Methodology	12

2. The Implementation Paradox	13
2.1 Availability and Access Do Not Equal Adoption	14
2.2 Institutional and Market Dynamics	15
2.3 Implementation Constraints Beyond Technology	15

3. Pillar 1: Data Governance and Interoperability	16
3.1 National Data Standards and Data Sharing	17
3.2 Data Protection and Trust	17
3.3 Addressing Agency Silos and Interoperability	18

4. Pillar 2: Digital Inclusion and Human Capacity **19**

4.1 Inclusion Beyond Coverage	20
4.2 The Non-Digital Barriers to Digital Life	20
4.3 Building Capacity and Closing the Talent Gap	21

5. Pillar 3: Cyber Resilience as a Public Good **23**

5.1 Citizen-Facing Trust and Safety	24
5.2 Critical Public Services and Continuity	26
5.3 Cyber Capacity and Regional Collaboration	26
5.4 Human Rights and Civic Space	27

6. Cross-Cutting Enablers **28**

6.1 Open-Source and Standards-Based Approaches in Practice	28
6.2 Modular Procurement Approaches	30
6.3 Delivery Capability and Operating Models	31
6.4 Regional Collaboration	32

7. The Roadmap: From Digital Presence to Digital Utility **33**

7.1 Strengthening Foundations	35
7.2 Integrating Systems	36
7.3 Expanding Utility and Regional Value	36
7.4 Short-, Medium-, and Long-Term Priorities Across All Tiers	37
7.5 Artificial Intelligence and Digital Foundations	38
7.6 Priority Use Cases Mapped to the Roadmap	39

8. Priority Areas for Development Partner Support **40**

8.1 From Projects to Public Capability 40

8.2 Areas Requiring Greater and More Sustained Investment 41

8.3 Effective interventions and sequencing support 42

8.4 Why This Matters for SIDS 42

9. Conclusion: Building Responsible Digital Foundations as a Development Imperative **44**

Endnotes **46**

Annex [A]: The Universal Digital Public Infrastructure (DPI) Safeguards Framework **49**

Annex [B]: Glossary of Terms **52**



Executive Summary

Digital progress in Small Island Developing States (SIDS) has advanced materially over the past decade, with wider connectivity, a growing number of digital strategies, and increasing experimentation in public services, digital payments, and identity-linked service delivery. This progress is marked by SIDS transforming into Small Island Digital States. The next phase of progress, however, depends not only on expanding digital presence but also on ensuring that digital ecosystems are holistically designed and capable of generating trusted, practical utility across interdependent sectors over time.

Drawing on UNDP's earlier SIDS digital work, a desk synthesis of 21 Digital Readiness Assessments (DRAs), stakeholder consultations, and selected evidence, including existing programmes in SIDS, this strategic brief highlights that the main constraints to robust digital scaling are increasingly institutional as much as technical. Fragmented data ecosystems, weak coordination, capacity gaps, low trust, and barriers to uptake outside the technology stack continue to slow implementation. These constraints are especially consequential in SIDS, where small populations, limited specialist capacity, dispersed geography, narrow vendor markets, and high exposure to climate and economic shocks can make fragmented or poorly governed digital investments more costly to sustain.

The brief outlines three mutually reinforcing pillars, supported by cross-cutting enablers:

- Data governance and interoperability
- Digital inclusion and human capacity
- Cyber resilience as a public good
- Cross-cutting enablers, including modular procurement, open-source and standards-based approaches, and public-sector delivery capability



An accompanying implementation-oriented roadmap is provided to help sequence policy, investment, and partnership choices across different starting points and levels of institutional readiness.

Key messages:

- SIDS are already demonstrating practical leadership across modernization, service integration, regional cooperation, open-source experimentation, and citizen-facing delivery models. Examples from Barbados, Trinidad and Tobago, Timor-Leste, the Dominican Republic, the OECS region, and Pacific contexts show that innovation is underway despite constraints.
- Non-technical barriers to building robust digital foundations include rigid, misaligned procurement processes that lag the rapidly changing digital world, institutional silos, weak coordination, low trust, skills gaps, and continuity risks. These barriers frequently slow progress, even when technical solutions exist or can be procured.
- Citizen-facing trust and safety are central to adoption, not merely a downstream concern. Trusted identity, interoperable data, skilled institutions, inclusive design, and resilient infrastructure, outlined as essential for advancing toward digital utility, are also preconditions for responsible AI adoption.
- For development partners, the most effective investments, programmes, and interventions strengthen implementation teams, data governance, adoption measures, continuity planning, and local ecosystems, alongside technology platforms.
- Building responsible digital foundations is essential for development. This brief provides SIDS leaders and partners with a practical pathway to move from digital presence to digital utility in ways that are more trusted, inclusive, and resilient.

Photo: Ministry of Digital Transformation Republic of Trinidad and Tobago

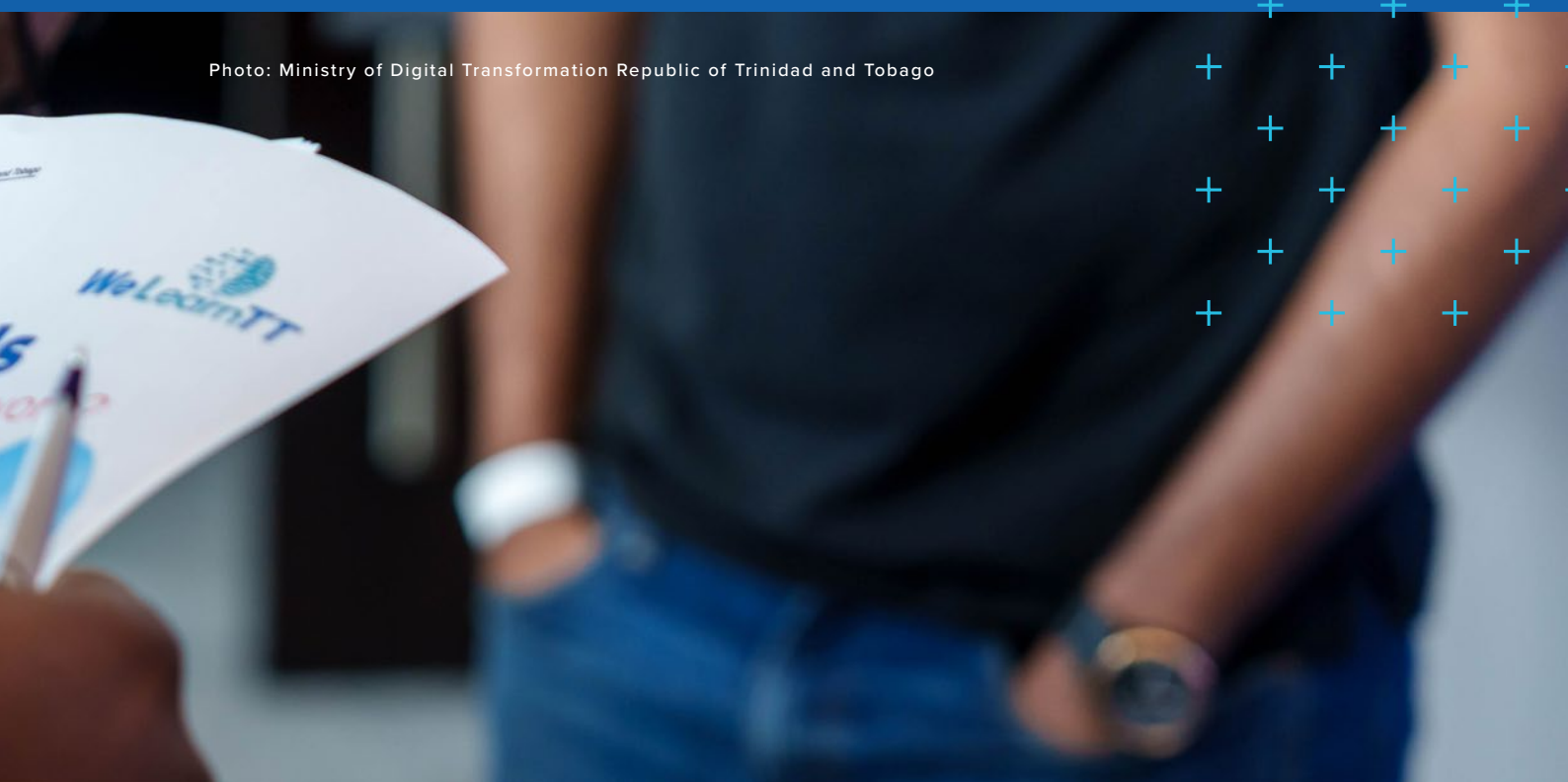




Photo: Ministry of Digital Transformation Republic of Trinidad and Tobago

1. Introduction and Context

Digital adoption can serve as a catalyst for inclusion, productivity, and resilience in SIDS, especially when there is a concerted emphasis on trust, utility, institutional capability, and continuity. The question is no longer only how digital can support development, but also what conditions are needed to build solid foundations for the adoption, governance, and sustained, trustworthy operation of digital systems over time.

Over the past several years, UNDP's work on system-based digital transformation in SIDS has shifted from broad diagnosis to more applied questions about building robust foundations, implementation, whole-of-society transformation, and scale. The earlier Small Island Digital States report demonstrated that digital technologies have the potential to improve service delivery, reduce geographic isolation, support entrepreneurship, and strengthen resilience. It identifies five pillars that shape national digital progress: connectivity, government, regulation, economy, and people. It also highlighted data exchange, digital legal identity, and digital payments as catalytic enablers.¹

The companion report on how digital is transforming the lives of young people in SIDS added an equally important people-centred perspective. Drawing on responses from more than 5,000 young people across more than 30 SIDS, it showed that building robust digital foundations and facilitating adoption is widely seen as a route to opportunity, connection, and creativity, but if designed and scaled without trust and safeguards, can also be a source of exclusion, harassment, scams, and uneven access.²

The Digital Readiness Assessment (DRA) is a country-level diagnostic framework that helps governments assess their readiness to use digital technologies for inclusive and sustainable development. It examines key dimensions of the digital ecosystem, including infrastructure, governance, the digital economy, skills, and public services, as well as cross-cutting areas such as data governance, cybersecurity, and inclusion. Drawing on stakeholder consultations and a mix of national and global data, the DRA identifies systemic gaps and opportunities, serving as a practical entry point for policy prioritization and investment in areas such as digital public infrastructure aligned with national development goals and the Sustainable Development Goals (SDGs).

A review of the 21 UNDP DRAs¹ that served as part of the evidence base for this brief, together with stakeholder consultations conducted in early 2026, reinforces three broad lessons:

- SIDS are already innovating, often under significant constraints.
- Many barriers to scale stem from the gap between policy intent and day-to-day implementation.
- The next phase of progress will increasingly depend on whether digital systems are trustworthy, integrated, and usable.

1.1 Latest Trends and Statistics

The digital context facing SIDS has changed substantially over the past decade. Connectivity has improved, but the challenge is no longer just getting people and government services online; it's about doing so meaningfully. Recent international data confirms both progress and persistent

¹ DRAs in the following countries have been reviewed for research purposes of this brief - Antigua and Barbuda, British Virgin Islands, Cook Islands, Cuba, Curaçao, Dominica, Grenada, Guinea-Bissau, Guyana, Haiti, Jamaica, Maldives, Mauritius, Nauru, Niue, Samoa, Solomon Islands, Suriname, Tonga, Trinidad and Tobago, and Tuvalu.

inequality. ITU's 2024 SIDS-focused analysis found that 67 percent of the population in SIDS was using the Internet in 2023, roughly double the level in 2014 and broadly in line with the world average. Growth has therefore been substantial, but it remains uneven across regions and between the urban and rural populations.³

- Internet use reached 75 percent in Caribbean SIDS, compared with 52 percent in African SIDS and 41 percent in Pacific SIDS.
- Urban-rural differences are significant: 84 percent of the urban population in SIDS uses the internet, compared with 44 percent of the rural population.
- Mobile broadband coverage remains incomplete, with 85 percent covered by 3G or above and a 15 percent coverage gap concentrated in Pacific SIDS.
- Affordability remains a material constraint. Among 50 SIDS with available data for data-only mobile broadband, only 18 met the Broadband Commission's affordability target in 2023. For fixed broadband, only 11 of 47 SIDS with available data met the target, and entry-level fixed broadband in a typical SIDS was about 46 percent more expensive than the world median.⁴

Beyond the coverage gap, a significant usage gap has emerged. ITU estimated that 18 percent of the population in SIDS had access to the Internet but did not use it, underscoring that affordability, devices, skills, trust, safety, and relevance now shape outcomes as much as network reach. For citizens entering the digital domain today, meaningful access increasingly depends on whether online environments and public services are understandable, safe, value-adding, and tied to services that people can trust and use.³

This matters especially because many new users are entering a digital environment very different from that of even five years ago. Today's digital environment and internet are shaped by platform concentration, which can manifest in SIDS as limited accountability and governance, a lack of local context and cultural specificity, limited user agency, and limited cultural inclusion. In addition, new digital users have to grapple with AI-enabled scams and fast-moving misinformation and disinformation, often with limited capacity, awareness, and tools at the local level to advance trust and safety or provide redress options.

Recent multilateral programming reflects these changing patterns and shifts in today's digital world. In addition to the SIDS reports highlighted in the introduction section, the Digital Pathways for SIDS 2.0 position paper from UNDP outlines digital pathways for transformation that encompass economic pillars such as digital business, open government, and digital government services and platforms, as well as elements of data privacy and cybersecurity. Global initiatives such as the Universal DPI Safeguards Initiative, stewarded by the UN Office for Digital and Emerging Technologies (ODET) and UNDP, place trust, inclusion, safety, and equity at the centre of digital transformation. In addition, the World Bank's Caribbean Digital Transformation Project tracks result not only in connectivity and systems deployment but also in digital public service uptake, e-money access, digital skills, affordability, business technology adoption, enterprise architecture, and

cybersecurity capacity. These shifts suggest that development partners increasingly understand digital transformation as a whole-of-system agenda linking infrastructure, institutions, adoption, and resilience rather than a narrow ICT rollout exercise.^{5,6}

1.2 Defining Digital Foundations and Digital Utility

For the purposes of this brief, responsible digital foundations are the minimum legal, institutional, technical, and human conditions required for digital systems to be useful, trusted, inclusive, and resilient over time. Broadly, this includes the following non-exhaustive but essential set of conditions:

- Citizens can reliably authenticate themselves to access services.
- Governments can share data safely across agencies.
- Institutions have the skills and authority to manage change.
- Services are accessible to those with low literacy, connectivity, low trust, or limited payment instruments.
- Public systems can continue to function during disruptions, including climate-related shocks and cyber incidents.



Photo: UNDP Guinea-Bissau

Trusted access, well-governed data re-use, practical user protection, and institutional coordination reinforce one another. The Universal DPI Safeguards Framework offers a practical lens through which these foundations can be operationalized. Its 18 foundational and operational principles, ranging from non-discrimination and agency to privacy- and security-by-design, inclusive governance, and effective remedy and redress, provide a common language for SIDS leaders and partners to coordinate action across the digital life cycle. The full list is provided in Annex A.

Digital utility refers to the ability of digital systems to generate trusted, practical, and sustained value for citizens, institutions, and public service delivery over time. It implies more than digital presence or technical deployment: systems must be usable, adopted, interoperable where necessary, inclusive, resilient, and embedded in institutional arrangements that allow them to function reliably in practice under operational, social, and environmental constraints.

1.3 Methodology

This brief draws on four main sources of evidence: UNDP's two previous SIDS digital reports^{1,2}; a desk synthesis of 21 UNDP Digital Readiness Assessments (conducted from 2020 to 2025)⁷; stakeholder consultations undertaken in early 2026 through a combination of expert interviews, questionnaires, and survey inputs from around 15 experts across Caribbean, Pacific, and other small-island contexts; and selected external research from ITU, the World Bank, OECD, and official government and publicly available sources.

The stakeholder consultations were intended to surface practical lessons, implementation constraints, and emerging examples rather than to provide statistically representative findings across all SIDS. The consultation evidence should be read as indicative and complementary to the broader DRA and secondary research base.





Photo: Mauritius and Seychelles Communications Team

2. The Implementation Paradox

The latest developments and stakeholder feedback for this brief suggest that digital transformation in SIDS is considerably more complex and layered than a technology challenge alone. In many cases, technical solutions exist or can be procured, yet digital outcomes still stall. The following scenarios are being observed:

- Portals or services are launched, but uptake remains low.
- Systems are built as one-off solutions rather than as modular, reusable foundations that can support continuous adaptation and innovation.
- Platforms are developed but remain weakly integrated.
- Digital channels are introduced, yet in-person services remain dominant.

These patterns point to a common underlying dynamic: digital investments designed and evaluated in isolation rarely generate the interdependencies needed for a sustainable, durable public utility. They also fail to connect clearly enough to the everyday value citizens look for: faster services,

predictable outcomes, fewer trips to offices, and transparency and fairness in how the system treats them. These implementation gaps often reflect three broader categories of risk operating in the background: risks to safety, risks to inclusion, and wider structural vulnerabilities, such as digital distrust, weak institutions, weak rule of law, and unsustainability.

2.1 Availability and Access Do Not Equal Adoption

Stakeholder feedback from across the Caribbean and Pacific consistently highlighted that the main challenge is not basic connectivity, but meaningful connectivity. This is a layered challenge: availability, i.e., the existence of connectivity or services, does not by itself produce access, which is determined by affordability, skills, usability, and safety conditions that enable people to actually use these services. Further, access does not by itself lead to adoption at scale because that is driven by citizens trusting these services and finding them relevant and useful. Some key patterns observed are below:

- In the **Dominican Republic**, connectivity has improved significantly and is broadly available, but access and meaningful use remain uneven due to differences in affordability, skills, device quality, geography, and public confidence and comfort with digital channels. Many citizens still prefer in-person services, not because digital channels are absent, but because awareness, confidence, and digital skills remain uneven.
- In **Dominica**, adoption of existing digital payments and services is constrained in part by limited access to formal banking instruments, such as ownership of banking cards. Addressing this could increase the uptake of digital payments by 20-30%.
- **Across four Pacific countries - Fiji, Tonga, Solomon Islands, and the Federated States of Micronesia**, the Pacific Digital Democracy Initiative found that digital adoption is constrained not only by skills, devices, or service design, but also by citizens' exposure to misinformation, technology-facilitated gender-based violence, and the limited reach of digital rights protections. The Pacific lesson is that "access does not equal adoption" extends beyond infrastructure and skills to the civic, rights, and safety conditions for participation.
- Consultation inputs from various contexts consistently highlighted interoperability gaps, limited public trust, and the absence of a sufficiently clear whole-of-government digital mandate as among the most significant barriers to progress. In practice, this refers to a lead entity or pan-government body with the authority and institutional capacity to convene across ministries, enforce common standards, and sustain implementation beyond electoral cycles. In many cases, the mandate exists formally but is not matched by the institutional structure or resources required to deliver on it. ⁸

2.2 Institutional and Market Dynamics

Implementation is also shaped by institutional and market dynamics that can be particularly consequential in small administrations where specialist capacity is limited, and a small number of institutions or vendors may play an outsized role in the digital ecosystem.

Consultations and research pointed to procurement rigidity, fragmented or unclear mandates, weak cross-ministry coordination, and, in some settings, vendor lock-in and concentrated market structures that can slow or complicate public-interest digital adoption.⁸

OECD's 2024 report on public-sector capacity strengthening in SIDS⁸ emphasizes that coordination demands, reporting burdens, specialist shortages, and compensation constraints often place small states at a disadvantage in managing reform. Similarly, the World Bank's 2025 report on digital public infrastructure⁹ and its analysis of unlocking DPI in Latin America and the Caribbean¹⁰ reinforce the same message: coordination arrangements, specialist capacity, and procurement flexibility shape outcomes as directly as the platforms themselves.

2.3 Implementation Constraints Beyond Technology

Across multiple country contexts, a consistent finding has emerged. Even where interoperability platforms or digital service portals have been established, broader digital utility still depends on service-provider ministries or departments' ability to redesign workflows, digitize internal processes, share data responsibly, and sustain implementation over time. Interoperability is not only a software issue; it is equally a question of operating models, governance, incentives, and administrative coordination.

Examples from the evidence base clearly illustrate this. In the Dominican Republic, a single citizen account has been funded and built, yet fuller deployment has faced challenges related to change management, uneven readiness across agencies, and resistance to data sharing. In Barbados, key digital health, identity, and e-services initiatives signal a strong intent to modernize but also highlight continuity risks associated with administrative transitions.

These experiences suggest that the next phase of digital transformation in SIDS will require greater attention to institutional incentives, public-sector delivery capabilities, process redesign, and adoption measures, alongside the technology stack.

The remainder of the brief examines three core pillars of responsible digital foundations - data governance and interoperability, digital inclusion and human capacity, and cyber resilience as a public good, followed by cross-cutting enablers such as procurement, delivery capability, open standards, and regional collaboration. Together, these sections will provide the basis for the implementation roadmap in section 7.



3. Pillar 1: Data Governance and Interoperability

In many cases across SIDS, core government services are still not fully digitized. These services within line ministries and the registries that underpin them remain paper-based, presenting a critical opportunity to design integrated, interoperable systems from the outset rather than retrofitting fragmented legacy infrastructure. Such interoperable systems should be grounded in common data standards, core registries, trusted authentication layers, auditability, and clear rules for access, consent, stewardship, and change management. Where these foundations are weak, each new system risks becoming another silo. Where they are stronger, interoperability becomes easier to scale, cheaper to maintain, and less dependent on custom point-to-point integration.

3.1 National Data Standards and Data Sharing

Fragmented data ecosystems are one of the principal barriers to effective and better service delivery from digital systems. When registries are duplicated, data standards vary, and ministries cannot reliably exchange information, governments face higher transaction costs, citizens are repeatedly asked for the same information, and confidence in digital services can erode. In SIDS contexts, to optimize for limited administrative bandwidth, the following levers need to be operationalized:

- Enabling national data standards, common definitions and minimum data-sharing protocols across priority registries like civil registration, tax, health and social protection.
- Introducing simple but enforceable agreements between agencies and departments on data access, use, and stewardship, and rules of exchange. In addition, clear escalation pathways, roles, and responsibilities should be outlined and aligned with resourcing and capacity realities to avoid overly complex and burdensome governance structures.
- Operationalizing consent-based data reuse, where users authorize specific data flows across agencies with visibility of what is shared. This can reduce repeated data entry and transactional friction while reinforcing user agency and trust, complementing rather than substituting for formal data-sharing agreements.

3.2 Data Protection and Trust

Across the DRA synthesis and stakeholder consultations, low levels of public trust repeatedly emerged as practical barriers to uptake, especially for identity-linked, cross-sector, or data-intensive services. Users and institutions alike are less likely to participate in digital exchanges when rules are unclear, safeguards are weak, or accountability for misuse is ambiguous, particularly concerning private and personal data. Data governance, therefore, needs to be treated as part of service design from the outset, not as a compliance layer added after systems are deployed. Open-source or standards-based adoption can support flexibility and reuse, but it still needs to be accompanied by safeguards, rights protections, and clear norms and inter-institutional rules governing how data is secured, accessed, shared, and audited.⁸

3.3 Addressing Agency Silos and Interoperability

Interoperability is often approached as a middleware or system-integration task. In practice, it is equally a governance challenge, one that involves incentive structures, institutional relationships, and feedback loops across agencies, not just technical integration between platforms. Consultation feedback, research and DRAs confirmed themes such as weak coordination, legacy systems that don't integrate smoothly, unclear mandates, and a lack of incentives for ministries to share information or jointly redesign processes.⁸

TIMOR-LESTE'S BALKAUN ÚNIKU PROGRAMME

Its institutional model links a multi-ministry governance structure, with the Ministry of State Administration as the executive body, line ministries as service owners, and municipalities as service providers. The initiative combines physical one-stop service centres, digital channels, and a municipal data agenda, demonstrating that coordination and accountability are prerequisites for interoperable service delivery rather than secondary features. Public reporting indicates that the model has already expanded across multiple municipalities and is reducing time, travel, and administrative burden for citizens. The broader lesson for SIDS is that interoperability becomes more viable when governance arrangements, delivery responsibilities, and service ownership are clearly structured from the outset.^{11,12,13,14}



Photo: UNDP Guinea-Bissau



Photo: Mauritius and Seychelles Communications Team

4. Pillar 2: Digital Inclusion and Human Capacity

Digital inclusion in SIDS is no longer well captured by coverage alone. As section 1 shows, internet use has grown markedly, yet access and use remain unequal across geography, income, age, and infrastructure contexts. The concept of inclusion is also evolving. In an environment shaped by generative AI, increasingly sophisticated scams, and pervasive misinformation and disinformation, inclusion must mean not only getting people online but also enabling them to engage safely, critically, and productively with digital systems. A key consideration for achieving this is to leverage familiar service delivery pathways. Rather than pushing entirely new platforms onto users for every new service, governments should integrate services into the channels citizens already know and trust. ^{2.3.15}

4.1 Inclusion Beyond Coverage

Meaningful participation depends on affordability, device access, language, accessibility, trust, and whether digital systems are designed around users' lived realities. Stakeholder input from across the Caribbean and the Pacific suggests that many people can access smartphones and basic internet services but remain less confident using formal digital channels for public services, finance, or administrative transactions. This confidence gap stems from the high stakes of formal transactions, concerns about data security, and the challenge of navigating complex digital interfaces. Digital inclusion should therefore be treated as a design principle and a capability agenda.⁸

Every major digital service should be designed with:

- User support and assisted channels, recognizing that not all citizens are able or willing to transact digitally without help. Assisted access means providing trained intermediaries at service centres, community offices, or post offices who can help citizens navigate digital services, particularly in rural and remote areas where travel time and limited connectivity create additional barriers.
- Multilingual and voice-enabled options where relevant, ensuring services are accessible in local languages and to those with limited literacy. This is particularly relevant in Pacific SIDS where high levels of linguistic diversity, for instance, with dozens or even hundreds of languages in Vanuatu, pose distinct challenges for inclusive and accessible digital systems. Advances in language AI create new possibilities here. UNDP's Local Language Partnerships Accelerator and related multilingual AI work illustrate how AI-enabled tools can support low-resource language communities, improve the efficacy of public communication – including in crisis contexts, and widen participation without compromising cultural specificity.^{16,17}
- Clear pathways for redressing grievances, sharing feedback, and accessing up-to-date information about the status of ongoing processes and files, so that citizens have recourse when digital services fail or produce errors.
- User-centred service design that accounts for travel time to digital centres where applicable, administrative friction, trust deficits, and the cost of digital access. This means moving beyond developing only the features of digital interfaces, focusing instead on user-friendly, intuitive workflows to reduce the fear of user error, with accessibility requirements in mind.

4.2 The Non-Digital Barriers to Digital Life

Some of the most important constraints on inclusion sit at the edges of the digital public infrastructure itself - in the adjacent systems, including payments, identity, accessibility, and assisted channels, that determine whether a digital service can actually be used. Similar barriers can arise around

foundational identity documents, disability access, limited confidence in public systems, or the absence of assisted channels. In some SIDS contexts, this is further compounded by the fact that segments of the population live in very remote or loosely connected settings, with some choosing to remain outside systems, meaning that incentives and context-sensitive approaches may be needed to prevent exclusion as public services are increasingly digitalized.

As highlighted in Section 2, consultations from Dominica underscored that when people lack access to bank accounts, debit cards, or other payment instruments, they may be unable to transact digitally even when digital financial services are available. A Pacific parallel is visible in Vanuatu, where the VANKLIA national payment platform and supporting regulatory arrangements are in place, yet everyday uptake remains low, illustrating the same point from a different angle: payment rails can exist before the broader conditions for routine use are in place.

In addition to UNDP's work on DPI in the Caribbean, the World Bank and Inter-American Development Bank's 2024 report on digital public infrastructure in Latin America and the Caribbean reinforces this point, emphasizing that digital financial inclusion, interoperable payment systems, and identity-linked service delivery are interdependent.¹⁰ Unlocking digital utility often requires addressing bottlenecks in adjacent systems that are themselves non-digital. Digital inclusion in SIDS, therefore, needs to be approached through a broader ecosystem lens that brings together finance, identity, accessibility, service design, and local trust.

4.3 Building Capacity and Closing the Talent Gap

SIDS face a human-capacity challenge across adoption and implementation. Citizens need the information, skills, and confidence to engage productively and safely with digital tools, while governments need implementers who can design, manage, procure, secure, and sustain digital systems. The shortage extends beyond developers to include product managers, enterprise architects, data stewards, procurement professionals, cybersecurity specialists, and public-sector delivery teams. OECD's 2024 report notes that brain drain can directly undermine the maintenance and sustainability of newly built capabilities by reducing institutional retention and continuity. In addition, Samoa, Jamaica, the Federated States of Micronesia, Haiti, Cabo Verde, Grenada, and Fiji are among the 20 countries that score the highest on the Human Flight and Brain Drain (HFBD) Index, which measures the economic impact of lost human capital.^{9,18}

To address these challenges, technical teams require robust training and capacity building; implementing institutions need to be directly involved in the scoping and design of new projects; public-sector job profiles need to be revised; and compensation needs to be adjusted to enable more competitive hiring and retention. The Dominican Republic has taken steps in this direction, but participants in the consultation acknowledged that trained staff frequently move to the private sector or to international organizations for higher pay.

BARBADOS – MODERNIZATION, DISCOVERABILITY, AND CITIZEN-FACING UTILITY

Barbados offers a useful example of how modernization can be linked to discoverability and usability rather than treated only as back-end digitization. Stakeholder inputs indicated progress across health, social services, immigration, and financial systems as part of a wider whole-of-government reform effort. They also highlighted regionally relevant examples such as re-use of travel-related service architecture across Barbados and Trinidad and Tobago, and civic-technology tools that make parliamentary information more searchable and usable for citizens. The lesson for SIDS is that inclusion is strengthened when modernization improves not only administrative efficiency, but also the visibility, navigability, and practical usefulness of public information and services.



SÃO TOMÉ AND PRÍNCIPE – MAPPING THE DIGITAL LANDSCAPE AS A FOUNDATION FOR CHANGE

São Tomé and Príncipe is similarly an example of how capacity building can serve as a deliberate entry point into broader digital transformation rather than a standalone intervention. A 2026 initiative targeting government decision-makers and university students combines digital and AI literacy with a structured effort to map existing data, AI, and digital public infrastructure initiatives, identify gaps, and connect discrete interventions to a wider portfolio aimed at rebuilding citizen-institution trust, advancing social justice, and creating sustainable economic opportunity. The lesson for SIDS is that the diagnostic and capacity-building phase, when designed with systems intent, can itself lay the groundwork for more coherent and legitimate digital transformation over time.



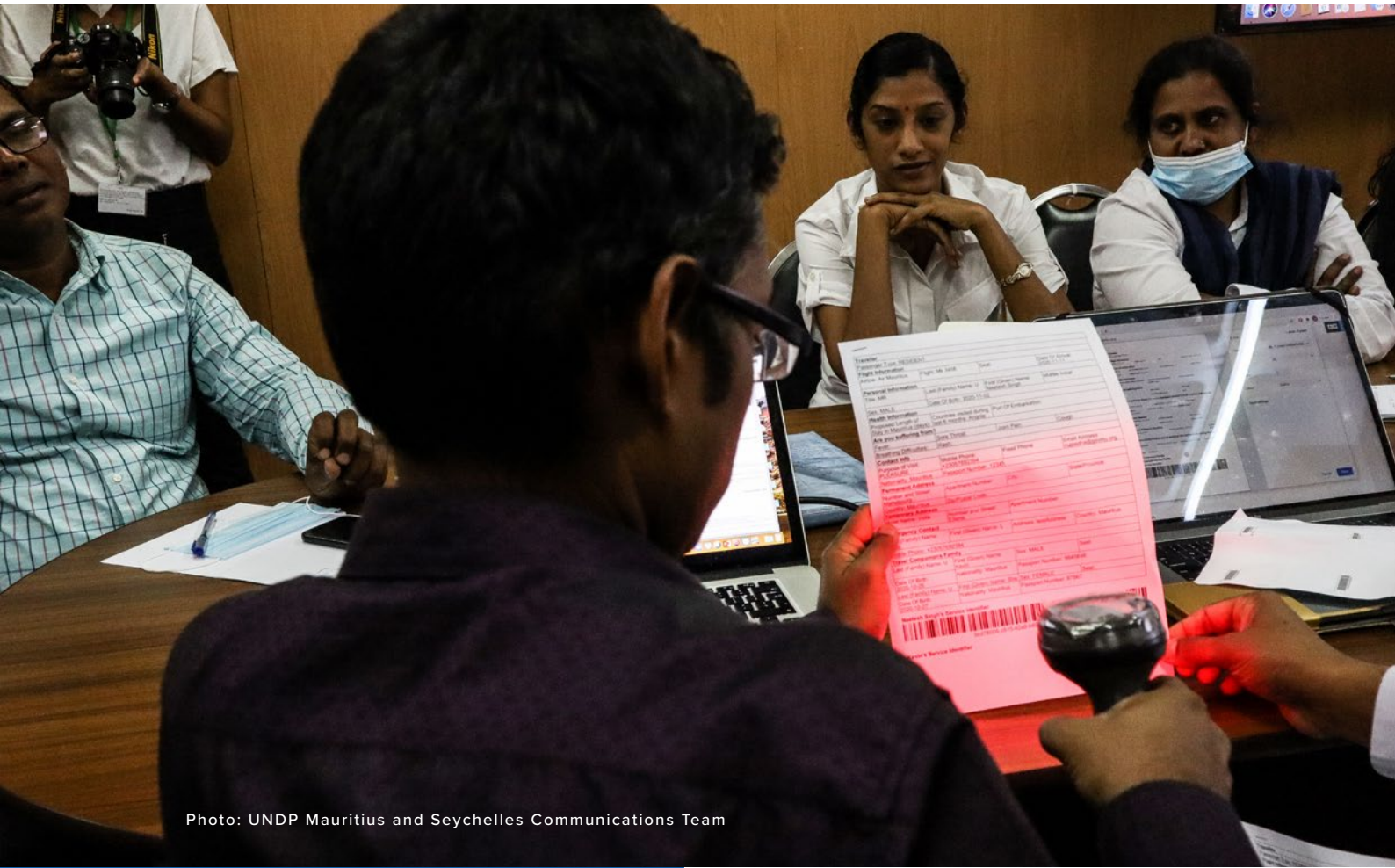


Photo: UNDP Mauritius and Seychelles Communications Team

5. Pillar 3: Cyber Resilience as a Public Good

For SIDS, cyber resilience encompasses more than just technical cybersecurity. The main focus is not only on protecting systems at the perimeter but also on ensuring that critical services remain operational and can recover swiftly after disruptions. This is particularly important in small island nations, where climate-related shocks, limited institutional capacity, reliance on external systems, and increasing exposure to scams and online risks often overlap.

5.1 Citizen-Facing Trust and Safety

Citizen trust depends not only on whether digital systems are secure, but also on whether people feel protected from fraud, scams, and harmful online behavior. This is increasingly urgent. A 2026 UNDP issue brief on digital scams frames scam operations as a significant development challenge, estimating that global financial losses are up to one trillion US dollars annually, equivalent to more than one per cent of global GDP, and with one in four persons worldwide falling victim.¹⁵ The impact is disproportionately severe in developing countries, where losses can reach 3-4 percent of GDP, institutional capacities for detection and consumer protection are often weaker, and rapid digital adoption risks outpacing available safeguards. The threat is compounded by advances in AI. Generative AI is increasingly embedded in scam operations across their lifecycle: before, during, and after the scam takes place.

A related observation from UNDP's work on AI Trust and Safety in small states is that AI is increasingly entering public-facing systems through the everyday tools officials and citizens already use, often without a formal adoption decision and without clear redress mechanisms. This reinforces why citizen-facing trust and safety belong in the foundational digital agenda.¹⁹

For SIDS, where many citizens are entering the digital domain for the first time, these risks are particularly acute. The earlier UNDP youth report found that many young people in SIDS were already concerned about scams, harassment, and other digital harms.² Stakeholder consultations highlighted the shortcomings of reducing cyber risk to cybersecurity, emphasizing that the goal should be broader public resilience covering people, governance, and behavior, not just technology.²⁰

Pacific consultation inputs raised a further dimension: the online harassment and bullying of female parliamentarians using digital platforms, with some Pacific countries lacking legal protections for female elected representatives in digital spaces. UNDP provides avenues for learning in this regard through its work with women MPs and parliamentary staff, developing safer reporting pathways, and supporting the Pacific Women in Power Forum, which connects parliamentarians across 14 countries for mentoring, solidarity, and skills-building.²¹

SINGAPORE'S EXPERIENCE IN BUILDING CITIZEN-FACING DIGITAL TRUST.

The approach operates at multiple levels simultaneously. At the ecosystem level, Singapore deploys detection and disruption systems, including the Scam Analytics and Tactical Intervention System (SATIS), that automate the identification and takedown of malicious websites and phishing operations. At the citizen-facing level, ScamShield provides a publicly accessible tool that helps users identify and block scam calls, messages, and links. Alongside these tools, Singapore maintains a strong public communications effort that frames scam prevention as a shared national responsibility rather than an individual burden. ²²

More broadly, Singapore's Singpass identity platform and MyInfo data service illustrate how trusted authentication and consent-based data reuse can reduce transactional friction while maintaining privacy safeguards. OpenAttestation adds a reusable, standards-based layer for verifiable digital documents. Taken together, these components demonstrate how trust can be built through a combination of institutional design, citizen-facing protections, and open trust infrastructure. The key lesson is that digital trust is strengthened when system security is paired with visible and practical protections that citizens can understand and use. ^{23, 24, 25}

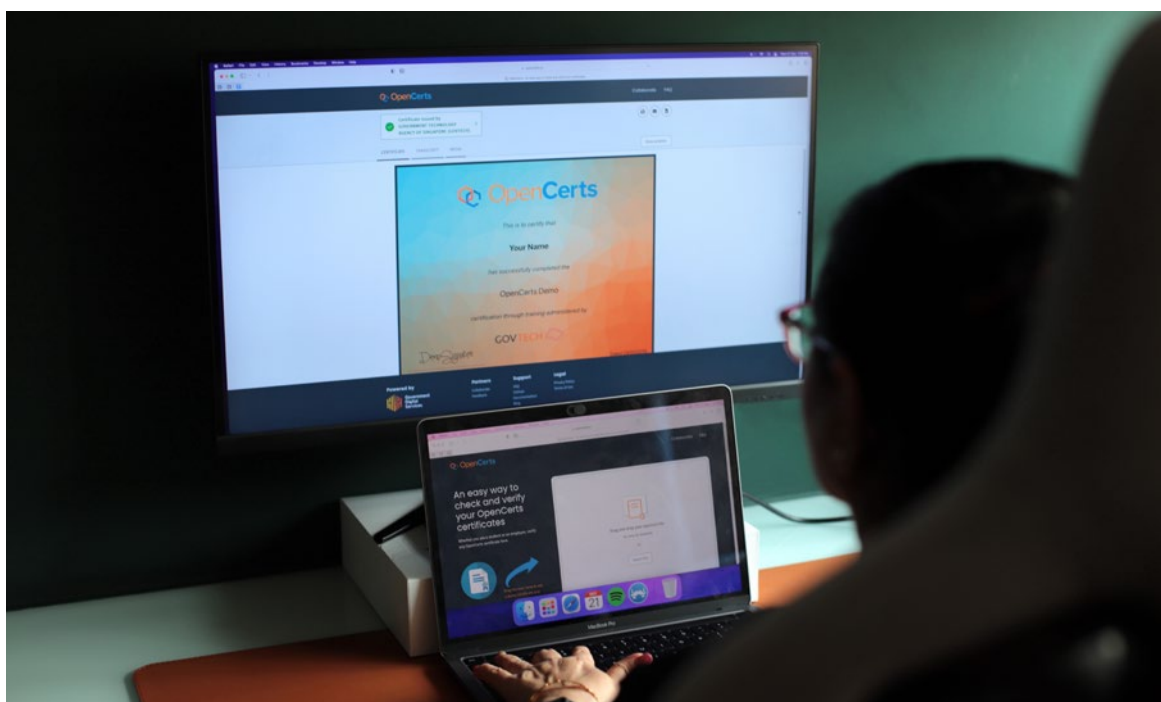


Photo: GovTech³⁵

5.2 Critical Public Services and Continuity

Identity systems, payment networks, registries, and health or social-protection platforms are increasingly vital as essential service layers. Disruptions can cause far-reaching effects beyond the ICT sector. Small populations, geographic factors, and reliance on few systems mean service outages can disproportionately affect SIDS. Therefore, disaster risk management, service resilience, and cyber readiness should be integrated into a single public-interest strategy with comprehensive contingency planning. Trinidad and Tobago's Digital Transformation Project, supported by UNDP, focuses on developing an electronic ID (e-ID) linked to the National Interoperability Framework, a National Trust Solution, and digital services across multiple ministries. The goal is to enhance the resilience, accessibility, and continuity of critical public services. ²⁶





5.3 Cyber Capacity and Regional Collaboration

The question of institutional form is especially important for microstates and smaller administrations. Some SIDS will benefit from lean national capabilities, supplemented by targeted regional collaboration, rather than attempting to replicate large, standalone cyber institutions.

The OECS region exemplifies how this approach can be implemented effectively. Through the World Bank-supported Caribbean Digital Transformation Project (CARDTP), Dominica, Grenada, Saint Lucia, and Saint Vincent and the Grenadines have initiated a coordinated Cybersecurity and Cybercrime Public Awareness Campaign. ²⁷ Conducted in partnership with CARICOM IMPACS and the OECS Commission, this campaign aims to provide citizens, institutions, and vulnerable groups, including the elderly, women, and rural communities, with the knowledge and resources needed to stay safe online. Simultaneously, these nations have collaborated with CARICOM IMPACS to develop a comprehensive Regional Cybersecurity Roadmap and to plan the creation of national Computer Incident Response Teams (CIRTs), with support from NRD Cyber Security. This integrated strategy focusing on awareness, capacity building, and regional cooperation serves as a promising example for small states. ^{28,29}

Cross-regional peer learning can further boost cooperation. For instance, the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE), active since 2019, has provided training on CERT operations, critical information infrastructure protection, and the use of international cyber norms to senior officials from ASEAN Member States and partner countries. Such arrangements—whether established regionally or accessed via existing facilities—offer a cost-efficient way for SIDS administrations to develop specialized skills without creating large, standalone institutions. ³⁰

Key considerations for effective regional cyber collaboration

-  Regional cooperation must account for the distinct circumstances of individual countries, including institutional scale, geography, and historical sovereignty considerations.
-  Collaboration is most likely to succeed when it complements, rather than overrides, national ownership.
-  Areas well-suited to regional cooperation include shared threat intelligence, joint capacity-building, harmonized legislative frameworks, coordinated public awareness campaigns, and pooled procurement of specialized expertise.
-  The conversation should encompass not only technical cybersecurity but also the resilience of public services, online harm, governance arrangements, and the well-being of citizens using digital systems.

5.4 Human Rights and Civic Space

A resilient digital environment must also protect human rights and civic participation and be open, transparent, participatory, and accessible. Cyber resilience protects not only infrastructure, but also civic trust and safe participation. Delivering on this vision requires robust policy, institutional, and regulatory frameworks that establish clear mandates, define responsibilities, and ensure enforceable legal standards. These formal frameworks are most effective when paired with support for community spaces, civil society organizations, and grassroots initiatives that lower practical barriers to participation and help citizens exercise their rights when systems fall short.



Photo: Ministry of Digital Transformation Republic of Trinidad and Tobago

6. Cross-Cutting Enablers

This section examines how open-source and standards-based approaches, modular procurement, delivery capability, and regional collaboration can serve as practical tools to support local ownership, adaptability, and value retention in SIDS digital ecosystems. For SIDS, these enablers are not generic reform measures; they are precisely the mechanisms that make small markets and thin administrative capacity viable along with reducing vendor dependence and stretching scarce expertise further.

6.1 Open-Source and Standards-Based Approaches in Practice

Open-source, interoperable, standards-based approaches can reduce vendor lock-in, support local customization, enable knowledge retention, and create space for genuine adaptation rather than wholesale replacement when a government changes or funding ends. This is especially relevant in small-state contexts, where long-term sustainability depends on avoiding systems that are difficult to maintain, integrate, or exit.

In practice, open-source is most useful when treated as part of a broader public digital architecture rather than as a standalone technology choice. For example, a government digitizing business registration, licensing, social protection enrolment, or municipal services may not need a single end-to-end proprietary platform. Instead, it may combine open-source or standards-based components for identity-linked access, form workflows, payments, notifications, registries, or verifiable documents, while requiring that each component works through common interoperability, security, and documentation standards.

In the Dominican Republic, the architecture around interoperability, citizen accounts, verifiable credentials, and digital payments has been deliberately framed around open standards and reusable components, including tools such as X-Road (interoperability), OpenG2P (cash transfer), Sunbird (verifiable credentials), and Inji (identity management). This technical approach is paired with institutional coordination, governance arrangements, and a clear public-interest rationale. Several of these components (e.g. X-Road, OpenG2P, Sunbird RC, and Inji) are registered Digital Public Goods (DPGs) under the DPG Alliance, alongside assets such as OpenAttestation. Engagement with the DPG ecosystem allows SIDS to draw from a curated, standards-compliant commons and, over time, to contribute their own context-adapted tools back to it.

TRINIDAD AND TOBAGO – INSTITUTIONALIZING OPEN-SOURCE ADOPTION³¹

Trinidad and Tobago illustrates both the promise and the challenges of open-source adoption in small-state settings. Stakeholder inputs described a gradual approach in which open-source is being used selectively across government and supported by an Open Source Programme Office intended to coordinate policy, licensing, compliance, and internal capability. At the same time, the approach is being shaped by legacy systems, network environments, procurement rules, and continuity risks associated with administrative change. The broader lesson is that open-source generates most value when it is backed by institutional stewardship, documentation, maintenance plans, and realistic transition pathways rather than treated as a one-off procurement choice. In small-state contexts, OSPOs also serve a knowledge-continuity function: by institutionalizing documentation, maintaining code repositories, and seeding know-how across the local ecosystem through partners and voluntary contributors, open-source approaches reduce the risk that critical technical expertise departs with individual staff.







6.2 Modular Procurement Approaches

Modular procurement approaches can help governments avoid overly rigid, monolithic systems that are difficult to adapt, maintain, or integrate with other services. Consultation findings highlighted several recurring challenges:

- Procurement frameworks often favor larger vendors, making it difficult for smaller domestic firms to provide support and customization services.
- Procurement timelines can be too slow and bureaucratic relative to political cycles and operational needs or misaligned with donor funding windows and timelines.
- Procurement reform is closely tied to how governments specify interoperability, manage supplier relationships, require documentation and knowledge transfer, and preserve viable exit options over time.

For a digital social protection system, modular procurement could break it down into the modules described in the table below.

Module 1 (Foundation)	Module 2 (Eligibility)	Module 3 (Payments)	Module 4 (User Interface)
 <p>Procure a standards-based identity verification service that connects to existing civil registration databases and uses open APIs.</p>	 <p>Contract separately for an eligibility rules engine, ensuring it integrates with Module 1 through documented interfaces.</p>	 <p>Rather than building custom infrastructure, procure integration with existing digital payment rails or mobile money platforms.</p>	 <p>Develop citizen-facing application and caseworker dashboards as distinct contracts, with requirements informed by user testing of earlier modules.</p>

This modular approach also creates opportunities for smaller vendors to compete and build smaller modules, since they may lack the resources to build the full system. However, in resource-constrained environments, modular approaches can entail a trade-off: each round of procurement carries its own administrative cost, which adds up quickly in small administrations and resource constrained settings. Recent UNDP-supported work with Pacific parliaments, including an LMS pilot and an LLM proof-of-concept procured through separate RFPs in Fiji and Yap, illustrates both the appeal of modular approaches to entering untested technology spaces and the administrative burden they impose on small teams.

In addition, UNDP's AI Trust and Safety work in small states highlights that two gaps increasingly determine whether new technologies, particularly AI-enabled systems, can be introduced into public services with adequate safeguards: unclear liability allocation in procurement contracts, and limited in-country capacity to independently test, audit, and monitor the systems being deployed. Modular approaches will only deliver on their promise if paired with serious investment in assurance capacity.

6.3 Delivery Capability and Operating Models

A common message from across the evidence base is that the success of digital systems depends heavily on the operating model that surrounds them. Governance arrangements, ministry coordination, service ownership, escalation pathways, service-level agreements, process redesign, vendor handover arrangements, user support, and continuity routines matter as much as the platform itself. In SIDS contexts, operating models need to be deliberately lightweight but clear: institutions should know who owns each service, who can require common standards, who resolves inter-agency issues, and how systems will be maintained beyond electoral cycles, donor windows, and vendor transitions.^{6,7}

VANUATU – BUILDING FOUNDATIONS TO SUPPORT TECHNICAL APPLICATIONS

Vanuatu's CRVS-to-ID-to-voter-roll sequence illustrates the brief's core lesson that foundations built in the right order create reusable public value across multiple public services. This effort was a part of the Vanuatu Electoral Environment Project (VEEP). Over several years, reforms to the civil registry, the identity layer, and the voter register were advanced sequentially rather than as isolated projects, with legal reform, institutional restructuring, and cross-ministry coordination proceeding alongside the technology development cycle. By 2023, National ID coverage among adults had become substantial, and the same identity infrastructure was already being used beyond elections, including in the COVID-19 vaccination campaign. The system was then stress-tested under crisis conditions during the January 2025 election. The broader lesson for SIDS is not electoral technology as such, but the value of sequencing: when civil registration, identity, legal architecture, and implementation capacity are built together, later applications - from social protection to labor mobility, health records, and disaster response become more credible and more reusable. There is also a lesson about realistic operational timeframes that can stretch to several years, which are often misaligned with unrealistic timelines anchored in technology solutioning alone.

6.4 Regional Collaboration

Regional collaboration can help reduce duplication, support common standards, and make scarce expertise more viable. At the same time, approaches must remain sensitive to differences in political economy, sovereignty concerns, and administrative scale. Regional approaches are most useful when they reduce duplication, preserve national agency, and focus on practical pain points rather than imposing a single model of cooperation. As highlighted in Section 5.3, regional collaboration on shared cybersecurity awareness campaigns and threat intelligence is a promising area. In addition, practical areas where regional collaboration has shown traction or holds promise include:

- Harmonized legislative frameworks for data protection, cybercrime, and electronic transactions.
- Joint procurement of specialist expertise and training, reducing per-country costs.
- Re-use of digital service designs and platforms across countries, as illustrated by the Barbados, Trinidad and Tobago travel platform.
- Regional centres of excellence for cyber capacity, enterprise architecture, and open-source stewardship.



Photo: Ministry of Digital Transformation Republic of Trinidad and Tobago

Photo: Mauritius and Seychelles Communications Team






7. The Roadmap: From Digital Presence to Digital Utility

This section translates recurring lessons from research and the insights highlighted above into an implementation-oriented roadmap. The purpose is to help sequence priorities, investment choices, and partnership strategies as countries move from digital presence to digital utility. Progress along this trajectory requires treating digital transformation as a systems challenge, where infrastructure, institutions, incentives, and inclusion interact and where gains in one dimension depend on conditions being met in others, all directed at generating concrete value for public service users. Progress also depends on attention to safeguards across the full lifecycle of digital systems from conception and scoping through design, development, deployment, and ongoing operations and maintenance, so that safeguards are built in rather than added as a layer later.

HOW TO READ THE ROADMAP

In line with the DRA approach, countries may be at different stages across different dimensions of digital development. A country may be relatively advanced in payments or digital identity, while remaining at an earlier stage in cyber resilience or multi-sector delivery capability. The pathways below are therefore intended to support sequencing and partnership design, not for ranking. Some of the technical terms in the table below are expanded on in the subsequent sections below.

Horizon	Strengthening foundations	Integrating systems	Expanding utility and regional value
Short term (0–2 years) 	Anchor rule of law, institutional capacity, recourse mechanisms; Stabilize core registries and trusted authentication; basic cyber hygiene; assisted access; priority service journeys	Establish data standards, reusable components, and initial secure exchange; reduce repeated data entry	Strengthen trust layers; pilot verifiable credentials and open APIs; deepen supplier assurance
Medium term (2–5 years) 	Expand service delivery; strengthen legal frameworks; build delivery teams and continuity routines	Integrate systems; operationalize interoperable exchange layers (middleware or service buses); redesign services around users	Advance regional collaboration; selected cross-border data and trade use cases; strengthen cyber cooperation
Long term (5+ years) 	Institutionalize capabilities and maintenance; deepen inclusive service access	Move toward proactive, data-informed service delivery; stronger safeguards	Lead in reusable trust infrastructure; advanced governance; selected regional public goods

Strengthening foundations is usually most relevant where one or more dimensions remain at basic or opportunistic stages; integrating systems becomes more relevant as countries move toward more systematic implementation; and expanding utility and regional value is most relevant where selected domains are already differentiating or approaching transformational maturity.

7.1 Strengthening Foundations

Key objective: Trust, simplicity, and service reliability.

Foundational priorities are most effective when guided by safeguards across the digital transformation lifecycle, so the building blocks established at this stage do not create exclusion, weak accountability, or security risks later. For countries that need to strengthen foundational conditions, the immediate priority is to establish a small number of reliable, trusted building blocks that create the conditions for multiple actors to build on them, so that scale, when it comes, is robust rather than brittle.

Key priorities include:

- **Conception and scoping:** Analyze the enabling environment for barriers to implementation and adoption, and anchor rule of law, institutional capacity, and recourse mechanisms early.
- **Rapid inventory of core systems and registries:** Identifying which databases, registries, and authentication systems exist, their condition, and their interoperability readiness. In practice, this means cataloging civil registries, tax databases, health records, and social protection systems, and establishing which are robust and functional.
- **A minimum viable trusted authentication path:** Enabling citizens to verify their identity through at least one reliable channel. This may start with a simple national ID verification linked to one or two high-demand services, such as social benefits or tax filing.
- **A manageable set of high-demand service journeys:** Rather than attempting to digitize all government services simultaneously, select two to three services with high citizen demand and clear process maps, such as birth registration, business licensing, or social protection enrollment, and ensure that the end-to-end user journey for a specific journey works smoothly.
- **Basic cyber hygiene and incident response:** Establishing foundational security practices across government networks, including regular patching, access management, and a basic incident response protocol.
- **Assisted digital access channels:** Providing trained intermediaries at community centres, post offices, or municipal halls who can help citizens navigate digital services. This is particularly important in contexts where digital literacy is low or trust in online systems is limited.

- **Procurement clauses that support interoperability and knowledge transfer:** Requiring vendors to deliver documentation, open data formats where feasible, and transition plans as standard conditions to proactively manage the risk.

7.2 Integrating Systems

Key objective: Turn disaggregated/fragmented digital assets into a coherent public utility.

For countries with fragmented digital assets, the next phase should focus on standards, cross-ministry governance, service integration, and adoption. Practical priorities include:

- **National data standards and secure data-sharing rules:** Defining common metadata schemas, unique identifiers, and consent-based sharing agreements that enable agencies to exchange data without duplicating registries.
- **An interoperable exchange layer for communication:** Deploying an interoperable exchange layer (middleware or service bus) that allows different government systems to communicate - for example, enabling a social protection agency to verify identity with a civil registry without building a custom integration each time.
- **Reusable components for authentication, payments, and notifications:** Building shared services that multiple agencies can use, reducing duplication and improving the citizen experience.
- **Capability building linked to active projects:** Training and mentoring staff through hands-on involvement in live implementation rather than through generic classroom exercises.

7.3 Expanding Utility and Regional Value

Key objective: Use stronger foundations to support innovation, interoperability, and regional learning rather than pursuing frontier technology without a structured strategy.

For countries that have already made progress in selected domains, the opportunity extends beyond domestic integration. Key priorities include:

- **Shaping reusable trust infrastructure:** Developing open APIs, verifiable credentials, and digital document standards that can be shared across government agencies and, in time, across borders.
- **Stronger supplier assurance and selected regional public goods:** Pooling expertise and resources with neighboring states to develop shared platforms, threat intelligence networks, or centres of excellence.
- **Piloting more advanced data governance and AI-readiness measures:** Where foundational trust and resilience are already in place, exploring how AI tools can enhance public service delivery, detection of fraud, or resource management while maintaining safeguards for responsible use.

7.4 Short-, Medium-, and Long-Term Priorities Across All Tiers

Across all three tiers:

- **Short term: Stabilize and unblock.** Fix high-friction bottlenecks, such as duplicate data-entry requirements, broken authentication pathways, or manual processes that deter citizens from completing transactions. Improve trust and usability and build minimum safeguards.
- **Medium term: Integrate and scale.** Align systems, operating models, legal frameworks, and capacity around a manageable set of high-value services, such as integrated social protection, digital payments for government transfers, health record interoperability, and business registration (depending on each country's priorities). These services demonstrate practical utility to citizens and build institutional confidence.
- **Long term: Sustain and optimize.** Institutionalize capabilities, move toward more proactive and data-informed services where appropriate, strengthen resilience, and enable stronger SIDS to support peer learning and regional public goods.

7.5 Artificial Intelligence and Digital Foundations

A discussion on digital foundations in SIDS would be incomplete without addressing the implications of AI. While AI tools can strengthen public service delivery, and as highlighted in Section 4.1, widen inclusion through multilingual and voice interfaces, SIDS are primarily adopters rather than developers of AI. UNDP's work on AI trust and safety shows that most SIDS lack the institutional capacity to independently evaluate the AI systems they deploy, and that those systems are rarely trained on local context or languages.

For SIDS, responsible AI adoption should be understood as a continuation of the digital foundations agenda rather than as a separate technology track. AI systems depend on the same enabling conditions that underpin digital utility: trusted identity, interoperable and well-governed data, resilient infrastructure, skilled institutions, inclusive design, and clear accountability mechanisms. Without these foundations, AI adoption risks amplifying existing fragmentation and biases as well as introducing new vulnerabilities. With them, SIDS can selectively and responsibly adopt AI, drawing on emerging frameworks for responsible AI governance and building reusable digital components that can support multiple ministries and, over time, be shared across SIDS. Emerging frameworks could include open, practically oriented tools such as Singapore's Model AI Governance Framework for Generative AI, released in 2024 and building on the earlier version; Singapore's Model AI Governance Framework for Agentic AI, launched in 2026; and AI Verify, an open-source AI governance testing framework stewarded by the AI Verify Foundation. ^{32,33}



Photo: UNDP Global Centre Singapore

7.6 Priority Use Cases Mapped to the Roadmap

Five priority use cases stand out from the current evidence base because they combine clear public value with feasibility across different readiness levels. Some are lower-complexity entry points that can help build trust and adoption early; others require stronger integration capacity but offer larger gains in efficiency, resilience, and institutional coordination.

- **Digital payments and financial inclusion (all tiers, near-term priority for foundation-builders):** Connecting service delivery, enterprise participation, and user uptake. For countries with low formal banking penetration, mobile money and simplified payment instruments offer a starting point.
- **Integrated public services and one-stop platforms (integrators and above):** Reducing the burden of repeated transactions for citizens and businesses. Timor-Leste's Balkaun Úniku model offers an instructive example of combining physical access points with digital interoperability.
- **Health and social-protection administration (integrators and above):** Strong candidates for identity-linked service delivery and data exchange, with high public demand and clear efficiency gains.
- **Civic and parliamentary tools (all tiers):** Strengthening transparency and participation. Barbados's parliamentary chatbot offers a low-cost, high-impact model that is replicable across the Caribbean and beyond by making parliamentary debates, legislation, and related records more searchable and easier for citizens and civil society to navigate.
- **Disaster and resilience systems (all tiers, acute priority for climate-vulnerable settings):** Increasingly important in SIDS settings where climate-related shocks, service continuity, and cyber preparedness intersect.





Photo: Ministry of Digital Transformation Republic of Trinidad and Tobago

8. Priority Areas for Development Partner Support

Development partners have an important role to play in the next phase of digital transformation in SIDS. The key shift is from treating digital primarily as a project or procurement category towards treating it as a capability and institutional transformation agenda.

8.1 From Projects to Public Capability

Public capability - the institutional ability to design, operate, govern, and continuously improve digital services is itself a development outcome, not a by-product of technology projects. Recognizing this requires development partners to confront a structural mismatch: traditional donor results cycles run two to five years, while the institutional change required to establish trusted digital foundations and achieve large-scale public adoption typically runs a decade or more.

Even in higher-capacity countries like Germany and the UK, foundational reforms around registries, digital identity, and interagency data sharing have taken years, sometimes more than a decade of legal, technical, and institutional iteration to gain traction. Expectations and timelines for resource-constrained SIDS should be calibrated accordingly: success should be measured against indicators of institutional consolidation and sustained service utility, not only against technology launch milestones.

8.2 Areas Requiring Greater and More Sustained Investment

Investment should begin at the identity, consent, and credentialing layer, including foundational identity, consent-based data reuse, and verifiable credentials, which underpins both current digital public services and responsible AI adoption. Without sustained investment at this layer, downstream use cases are harder to scale safely, and AI-enabled services in particular cannot be deployed with the consent provenance, credential verification, and auditable identity binding that responsible adoption requires.

Around this foundation, five institutional capability areas recur across the evidence base as requiring stronger and more sustained partner investment:

- **Implementation teams and digital delivery capability:** Funding for product managers, data stewards, and delivery specialists embedded within government, not only external consultants.
- **Data governance and stewardship:** Support for data standards, registries, privacy frameworks, and the institutional arrangements that sustain them.
- **Procurement modernization and interoperability support:** Technical assistance for modular procurement, open-standards requirements, and knowledge-transfer clauses.
- **User adoption, communication, and assisted access:** Investment in the demand side of digital services, including digital literacy, trust-building campaigns, and intermediary channels.
- **Continuity and resilience planning for critical digital services:** Support for business-continuity plans, disaster-recovery arrangements, and regional cyber collaboration.

8.3 Effective interventions and sequencing support

These investments are most effective when designed as a system rather than as isolated technical inputs. Three principles should shape how development partner support is designed, sequenced and delivered:

- **Sequencing by institutional readiness:** Foundational layers, particularly identity, consent, and basic data protection should precede or accompany sectoral applications rather than being retrofitted after vertical systems have already been deployed.
- **Bundling technology with the capability to operate it:** Platform investments should be paired with the delivery units, legal and regulatory support, governance frameworks, and adoption measures on which they depend, funded together, not in separate windows or by separate partners.
- **Designing for continuity beyond product launches:** Programming should explicitly fund maintenance, knowledge transfer, and local stewardship arrangements beyond initial deployment. Standards-based and open-source components strengthen this package only where procurement, documentation, and long-term stewardship arrangements are in place to support them.

8.4 Why This Matters for SIDS

The cost of fragmented or abandoned systems is particularly high in small states with constrained fiscal space and thin administrative capacity. Small populations make maintenance failures and institutional duplication more expensive per user, while geographic isolation, exposure to shocks, and limited labor markets make resilience and retention more difficult.

Digital transformation financing in SIDS should therefore be assessed not only against technology launch milestones but also against indicators of long-term utility: service usage, citizen trust, adoption of interoperability, continuity capacity, retention of local capabilities, and institutions' ability to govern systems beyond vendor contracts. These can be complemented by a small set of people-centred safeguard indicators that measure impact on users, not only on systems: (i) the percentage of DPI-related services that offer alternative or analog access channels for those who cannot transact digitally; (ii) the percentage representation from across society, including women, persons with disabilities, rural communities, and other underserved groups, in the design and review of major digital systems; and (iii) the number and types of mechanisms available for effective and timely redress when systems fail. Drawing on the Universal DPI Safeguards Framework, these indicators turn safeguards from aspiration into something partners and governments can track and fund.

What partners can support by tier:

- **Strengthening foundations:** foundational safeguards assessments, technical assistance for registries, identity systems, and basic authentication; procurement reform and knowledge-transfer requirements; basic cyber hygiene and incident-response capacity; assisted access infrastructure and digital literacy measures; and support for foundational data protection legislation.
- **Integrating systems:** co-funding of interoperability layers and service buses; delivery units and embedded technical teams; service redesign and user-centred design support; data governance frameworks and institutional coordination mechanisms; and capacity building tied directly to live implementation.
- **Expanding utility and regional value:** seed funding for regional public goods such as shared threat intelligence, centres of excellence, and reusable trust infrastructure; advanced governance frameworks for data, AI, and cross-border services; support for open-source stewardship and regional knowledge exchange; and selective piloting of responsible AI applications in public service delivery.



Photo: Samory Araújo/PNUD-AccLab Cabo Verde



Photo: Ministry of Digital Transformation Republic of Trinidad and Tobago

9. Conclusion: Building Responsible Digital Foundations as a Development Imperative

SIDS continue to demonstrate their capacity for digital innovation despite constraints. For SIDS, this is not only a question of modernization but of scale, resilience, and localized self-reliance – i.e. building digital systems that small administrations can govern, maintain, adapt, and trust over time. The evidence assembled for this brief demonstrates ambition, practical experimentation, and a growing willingness to adopt standards-based and citizen-centred approaches. The

question is no longer only how to increase digital presence, but how to ensure that digital investments cohere into trusted, useful, inclusive, and resilient systems, rather than accumulating as fragmented infrastructure.

Responsible digital foundations should therefore be treated as a development imperative. Data governance, inclusion, capacity, cyber resilience, modularity, and delivery capability are the conditions under which digital transformation can support sustainable development at scale. Without these foundations, digital investments may remain fragmented, underused, or vulnerable. With these foundations in place, SIDS can accelerate service delivery, strengthen resilience, expand participation, and create more durable pathways into the digital economy.

A forward-looking agenda should build on the strengths already visible across the SIDS community:

- **Barbados** demonstrates the value of modernization coalitions and regional discoverability, including replicable civic-technology tools and cross-country service reuse.
- **Trinidad and Tobago** demonstrates practical experimentation with open-source tools and institutional innovation in open-source governance.
- **Timor-Leste** demonstrates that one-stop public services, municipal data systems, and service integration can be linked to decentralization and local empowerment, reaching more than 18,400 citizens across multiple municipalities.
- **Vanuatu** demonstrates that digital foundations designed around citizenship, inclusion, and continuity, not only transactional efficiency and codified through legislation, can create reusable public value across elections, health, and other services.
- **The Dominican Republic** demonstrates that standards-based digital public infrastructure can advance through pragmatic institutional reform and sequencing.
- **Dominica** demonstrates the importance of addressing the real barriers to uptake, including financial inclusion and user confidence.
- **Fiji** demonstrates that cyber resilience in SIDS must be understood as a public good linked to safety, continuity, and well-being, and not only as a technical cybersecurity function, such as enshrining protections for vulnerable populations in the National E-Commerce Strategy.³⁴
- **São Tomé and Príncipe** illustrates that the journey toward responsible digital foundations can begin with deliberate capacity building and systems mapping, connecting digital literacy to a larger vision of institutional trust and social transformation.
- **The OECS region** demonstrates how coordinated regional approaches to cybersecurity, public awareness, and institutional capacity can be achieved through collaborative frameworks such as CARDTP.

Taken together, these experiences suggest that the next phase of SIDS digital transformation is already underway. SIDS leaders and partners, especially donors, multilateral development banks, and investors, can use this brief and its evidence base to help move SIDS from digital presence to digital utility.

Endnotes

- 1 United Nations Development Programme (UNDP), Small Island Digital States: How Digital Can Catalyse SIDS Development, 2024. Available at: <https://www.undp.org/publications/small-island-digital-states-how-digital-can-catalyse-sids-development>
- 2 UNDP, How Digital Is Transforming the Lives of Young People in Small Island Developing States, 2024. Available at: <https://www.undp.org/publications/how-digital-transforming-lives-young-people-small-island-developing-states>
- 3 International Telecommunication Union (ITU), Measuring Digital Development: Facts and Figures: Focus on Small Island Developing States, 2024. Available at: https://www.itu.int/hub/publication/d-ind-ict_mdd-2024-1/
- 4 ITU, Measuring Digital Development: Facts and Figures 2024. Available at: <https://www.itu.int/itu-d/reports/statistics/facts-figures-2024/>
- 5 World Bank, Caribbean Digital Transformation Project (P171528), project page and appraisal materials, 2020. Available at: <https://projects.worldbank.org/en/projects-operations/project-detail/P171528>
- 6 World Bank, Caribbean Digital Transformation Project (P171528), Implementation Status and Results Report, February 2025. Available at: <https://documents1.worldbank.org/curated/en/099021825090536460/pdf/P171528-57158ae9-a7ed-4f3a-93a5-82cf34215f70.pdf>
- 7 UNDP Digital Readiness Assessments for 21 SIDS, desk synthesis notes, and Stakeholder consultation and feedback.
- 8 OECD, Improving Public Sector Capacity-Strengthening Support for Small Island Developing States, 2024. Available at: https://www.oecd.org/en/publications/improving-public-sector-capacity-strengthening-support-for-small-island-developing-states_aec0effa-en.html
- 9 World Bank, Digital Public Infrastructure and Development: A World Bank Group Approach, 2025. Available at: <https://openknowledge.worldbank.org/entities/publication/cca2963e-27bf-4dbb-aa5a-24a0ffc92ed9>
- 10 World Bank and Inter-American Development Bank, Unlocking the Potential of Digital Public Infrastructure in Latin America and the Caribbean, 2024. Available at: <https://openknowledge.worldbank.org/entities/publication/ed8d0ed7-824d-4581-acf4-65fbad0f651d>
- 11 UNDP Timor-Leste, Bringing Public Services Closer: Balkaun Úniku materials and related news releases, 2024–2026. Available at: <https://www.undp.org/timor-leste/stories/bringing-public-services-closer-people>
- 12 UNDP Timor-Leste, “Bringing Public Services Closer: Balkaun Úniku Expands to More Municipalities, Empowering Timorese Citizens,” 2025. Available at: <https://www.undp.org/timor-leste/news/bringing-public-services-closer-balkaun-uniku-expands-more-municipalities-empowering-timorese-citizens>

- 13 Balkaun Úniku official website and service materials, 2024–2026. Available at: <https://balkaununiku.gov.tl/en/>
- 14 Timor-Leste Municipal Portal / Data Platform for the Development of Timor-Leste. Available at: <https://portal.municipio.gov.tl/en/>
- 15 UNDP, Countering Digital Scams: Stemming the Tide on an Urgent Development Challenge, 2026. Available at: <https://www.undp.org/publications/countering-digital-scams-stemming-tide-urgent-development-challenge>
- 16 UNDP AI Hub for Sustainable Development, Local Language Partnerships Accelerator. Available at: <https://www.undp.org/digital/ai/local-language-partnerships>
- 17 Dr. Kyungho Song & Dr. Jiyeon Cho, Korea AI Safety Institute, Alena Klatté, Jennifer Louie & Barbora Bromová, UNDP Digital, AI and Innovation Hub, Building Safer AI for All Languages: A Collective Pathway to Inclusive Human Development. Available at: <https://www.undp.org/digital-innovation/blog/building-safer-ai-all-languages-collective-pathway-inclusive-human-development>
- 18 Fund for Peace (2024). [Human flight and brain drain by country, around the world | TheGlobalEconomy.com](https://www.fundforpeace.com/reports/human-flight-and-brain-drain-by-country-around-the-world/)
- 19 UNDP, upcoming report on “Small states, AI diffusion: how lessons from Small Island Developing States and Low and Middle-Income Countries can shift the future of AI Trust, Safety, and System Performance Globally”
- 20 Freedom House, Timor-Leste: Freedom in the World 2024 Country Report. Available at: <https://freedomhouse.org/country/timor-leste/freedom-world/2024>
- 21 UNDP, Democracy’s Blind Spot: Technology-Facilitated Violence Against Our Women Leaders. Available at: <https://www.undp.org/pacific/blog/democracys-blind-spot-technology-facilitated-violence-against-our-women-leaders>
- 22 GovTech Singapore and ScamShield resources on scam prevention, including ScamShield and SATIS. Available at: <https://www.tech.gov.sg/products-and-services/for-citizens/scam-prevention/>
- 23 Singapore Government Developer Portal, Singpass overview and related Myinfo materials. Available at: <https://www.developer.tech.gov.sg/products/categories/digital-identity/singpass/overview>
- 24 OpenAttestation official documentation and overview. Available at: <https://www.developer.tech.gov.sg/products/categories/blockchain/openattestation/overview> <https://openattestation.com/>
- 25 Smart Nation Singapore official resources. Available at: <https://www.smartnation.gov.sg/>
- 26 UNDP, The Trinidad and Tobago Digital Transformation Project. Available at: <https://www.undp.org/trinidad-and-tobago/projects/trinidad-and-tobago-digital-transformation-project>
- 27 OECS Commission / CARICOM IMPACS, CARDTP Cybersecurity and Cybercrime Public Awareness Campaign, 2025. <https://caribbean.eclac.org/node/4878>

- 28** World Bank, Digital First Responders: The Role of Computer Security Incident Response Teams (CSIRTs) in Developing Countries, 2024. Available at: <https://openknowledge.worldbank.org/entities/publication/4187c872-2053-43bc-9a47-fbaeb33b74e7>
- 29** World Bank, Strengthening Cybersecurity and Resilience of Critical Infrastructure: Insights from the Republic of Korea and Other Digital Nations, 2025. Available at: <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099705012152346616>
- 30** ASEAN – Singapore Cybersecurity Centre for Excellence (ASCCE) <https://cybilportal.org/projects/asean-singapore-cybersecurity-centre-for-excellence-ascce/>
- 31** UNDP, “New Open Source Programme Office In Trinidad and Tobago Sets Out To Catalyze Digital Public Services”. Available at: <https://www.undp.org/digital/news/new-open-source-programme-office-trinidad-and-tobago-sets-out-catalyze-digital-public-services>
- 32** IMDA and AI Verify Foundation, 2024. Model AI Governance Framework for Generative AI. Available At: <https://aiverifyfoundation.sg/wp-content/uploads/2024/06/Model-AI-Governance-Framework-for-Generative-AI-19-June-2024.pdf>
- 33** IMDA, 2026. Model AI Governance Framework for Agentic AI. Available At: <https://www.imda.gov.sg/-/media/imda/files/about/emerging-tech-and-research/artificial-intelligence/mgf-for-agentic-ai.pdf>
- 34** Republic of Fiji, National E-commerce Strategy 2025–2029. Available at: <https://www.mcttt.gov.fj/wp-content/uploads/2025/04/Fiji-National-E-Commerce-Strategy-2025-2029.pdf>
- 35** UNDP, Why Singapore is building digital public goods. Available at: <https://www.undp.org/blog/why-singapore-building-digital-public-goods>

Annex [A]: The Universal Digital Public Infrastructure (DPI) Safeguards Framework

The Universal DPI Safeguards Framework has been developed by the DPI Safeguards initiative, a global multi-stakeholder effort convened and supported by the UN Office of Digital and Emerging Technologies (ODET) and the United Nations Development Programme (UNDP). It is designed to ensure that digital infrastructure (such as digital ID, data exchange layers, and payment systems) is built and operated safely and inclusively.

The principles listed in the Framework are shaped by various research methods, including consultations with diverse stakeholders, a review of secondary resources, case study analysis and discussions with country-based implementers. As the DPI landscape evolves, these principles should be periodically reviewed and updated. By adopting these 18 principles as a baseline for national policy and regional public procurement, SIDS can rapidly deploy secure, equitable, and accountable digital foundations.

The principles are divided into two categories: (1) foundational and (2) operational. The former refers to principles that should serve as the basis for any DPI, while the latter refers to principles that come into play at an operational level and may vary across contexts.

Foundational principles: The building blocks for safe and inclusive DPI

- F1. Do no harm: A human rights-based framework should be integrated throughout the DPI life cycle to anticipate, assess, and effectively mitigate any potential human rights harms and power differentials.
- F2. Do not discriminate: All individuals, regardless of intersecting identities, should have unbiased access and equal opportunity.
- F3. Do not exclude: All individuals should have a choice of channels (digital/non-digital) to access and benefit from services enabled by DPI based on their individual capacity and resources.
- F4. Reinforce transparency and accountability: DPI should be developed with democratic participation, have public oversight, promote fair market competition and avoid vendor lock-in. All partnerships should be transparent, accountable and publicly governed.
- F5. Uphold the rule of law: DPI should be introduced with a clear legal basis, with required legal and regulatory aspects embedded into its design, supported with capacity for sector specific tailoring (such as health), implementation, oversight and regulation by law.

- F6. Promote autonomy and agency: Ensure that everyone (especially indigenous communities with sui generis rights), on their own or with assistance, can take control of their data, promote their agency, exercise choice, and contribute to their society's well-being.
- F7. Foster community engagement: All stages of the DPI life cycle should centre on the needs and interests of individuals and communities at risk. They should participate at critical junctures and provide feedback actively in an environment of transparency and trust.
- F8. Ensure effective remedy and redress: Complaint response and redress mechanisms, avenues for appeal without reprisal, supported by robust administrative and judicial review, should be accessible to all in a transparent and equitable manner during service delivery.
- F9. Focus on future sustainability: Inculcating foresight is key to anticipating and limiting long term and inter-generational harms.

Operational principles:

Driving continuous trust and adaptation

- O1. Leverage market dynamics: DPI should foster an increasingly inclusive environment for public and private innovation such that market players can compete and introduce diverse equitable solutions that cater to emerging needs of all people across the society.
- O2. Evolve with evidence: Independent, transparent, and continuous assessments, due diligence, or audits should engage with people, understand concerns, review evidence and rapidly cease or initiate activities that contain heightened risks or harms.
- O3. Ensure data privacy by design: DPI should embed legal, regulatory and technical principles that enforce core privacy principles (e.g., data minimization, provisions to delink, ability to limit observability) and legal safeguards should be enacted around them.
- O4. Assure data security by design: DPI should incorporate and continually upgrade security measures, such as encryption or pseudonymization, to protect personal data. A legal framework should fill the gaps where technical design may be insufficient for data security.
- O5. Ensure data protection during use: Personal data should be processed or retained lawfully and transparently only by authorized personnel within a legal framework including transaction history, data subject rights and protections against overreaching requests.
- O6. Respond to gender, ability or age: Not all individuals experience DPI in the same way, and some continue to face barriers and challenges related to access or use. DPI implementation should not exacerbate existing challenges or introduce new barriers and inequalities.

- O7. Practise inclusive governance: Long-term effectiveness of DPI is contingent upon the establishment of a robust legal, regulatory and institutional framework that should promote transparent and participatory multi-stakeholder governance focused on safety and inclusion.
- O8. Sustain financial viability: As DPI are a public infrastructure, diversified, phased and sustainable financing models should be established. Governments can lead during the build phase and local digital partners, or the private sector can lead on operations and maintenance.
- O9. Build and share open assets: DPI should share and reuse open protocols, specifications, Digital Public Goods (DPGs), and the associated knowledge. This enhances flexibility and assures that proprietary systems do not limit the ability to improve safety and inclusion.
- These principles should integrate with various stages of the DPI life cycle, otherwise they risk remaining as philosophical statements. The Framework translates these principles into processes and illustrates them with observed practices so that they can be contextualized and implemented by the responsible authorities.



Annex [B]: Glossary of Terms

This glossary defines technical, institutional, and programme-specific terms used in this brief. It is intended as a reference for readers across policy, technical, and operational backgrounds, and is not exhaustive. Terms are ordered alphabetically.

API (Application Programming Interface) - A defined set of rules through which one software system requests services or data from another. In a public-sector context, open APIs are those published under terms that allow approved third parties, including other government agencies, vendors, or civil society, to integrate with government systems without bespoke, case-by-case arrangements.

Assurance (in AI systems) - The set of technical and institutional practices used to establish that an AI system behaves as intended, including independent testing, auditing, monitoring, and documentation. Assurance is the bridge between procurement and safe deployment.

Balkaun Úniku - Timor-Leste's one-stop public services programme, combining physical service centres, digital channels, and a municipal data agenda under a multi-ministry governance arrangement. Referenced in Section 3.3.

CARDTP (Caribbean Digital Transformation Project) - A World Bank-supported programme operating across OECS states that supports digital government, service delivery, and cybersecurity, including the Cybersecurity and Cybercrime Public Awareness Campaign referenced in Section 5.3.

CARICOM IMPACS - Caribbean Community Implementation Agency for Crime and Security. The regional security coordination body responsible, among other mandates, for cybercrime and cybersecurity cooperation across CARICOM member states.

CIRT / CSIRT - Computer Incident Response Team (also Computer Security Incident Response Team). A standing function responsible for detecting, coordinating response to, and recovering from cyber incidents affecting critical systems.

CRVS (Civil Registration and Vital Statistics) - The continuous recording of vital events births, deaths, marriages and related demographic data. A functioning CRVS is a foundational input to identity, social protection, health, and electoral systems, as illustrated by the Vanuatu sequencing example in Section 6.3.

Enterprise architecture - The documented arrangement of an organization's processes, data, applications, and infrastructure, together with the rules for how they fit together. In government, a functioning enterprise architecture capability is what turns individual ICT projects into coherent systems.

Inji - An open-source mobile identity wallet, developed within the MOSIP ecosystem, that allows users to store and present verifiable credentials from identity and other providers. Referenced in the Dominican Republic example in Section 6.1.

Interoperable exchange layer (middleware, service bus) - A shared technical layer that allows separate government systems to exchange data securely without building direct, custom integrations between each pair of systems. Common implementations include message-bus architectures and federated exchange platforms such as X-Road.

Metadata standards - Common definitions for how data fields are labeled, structured, and described across systems. Shared metadata is a precondition for reliable data exchange and a recurring foundation for interoperability.

MyInfo - A consent-based personal-data service operated by the Government Technology Agency of Singapore, which allows residents to reuse pre-verified personal data when applying for government and private-sector services, reducing repeated data entry. Referenced in Section 5.1.

OEDT (UN Office for Digital and Emerging Technologies) - The UN entity with system-wide responsibility for digital and emerging-technology policy coordination, and joint steward — with UNDP — of the Universal DPI Safeguards Initiative.

OECS (Organisation of Eastern Caribbean States) - A nine-member regional body whose members are predominantly small island states that cooperate on economic, digital, and cyber policy, including through shared institutions and joint programmes such as CARDTP.

OpenAttestation - A Singapore-developed, open-source framework for issuing and verifying tamper-evident digital documents and credentials, using public-key cryptography and anchoring on distributed ledgers. Used across certificates, licenses, and other official records.

OpenG2P - An open-source set of components supporting government-to-person (G2P) payment programmes, covering beneficiary enrolment, payment disbursement, and reconciliation. Referenced in the Dominican Republic example in Section 6.1.

SATIS (Scam Analytics and Tactical Intervention System) - A Singapore Government capability that automates the identification and takedown of malicious websites and phishing operations. Referenced in Section 5.1.

ScamShield - A Singapore public-facing application that helps users identify and block scam calls, messages, and links. Referenced in Section 5.1.

Singpass - Singapore's national digital identity and authentication service, used to access a wide range of public and private services. Referenced alongside MyInfo in Section 5.1 as an illustration of trust-anchored authentication paired with consent-based data reuse.

Sunbird RC - An open-source platform for building electronic registries, supporting use cases such as health records, education records, and verifiable-credential issuance. Referenced in the Dominican Republic example in Section 6.1.

VANKLIA - Vanuatu's national retail payment platform, operated in conjunction with supporting regulatory arrangements. Referenced in Section 4.2 to illustrate that payment infrastructure can exist in advance of the broader conditions for routine use.

Verifiable credentials - Digital credentials such as qualifications, permits, or identity attributes that can be presented and cryptographically verified without contacting the issuing authority each time. Verifiable credentials are a building block for re-usable digital identity and credentialing and underpin several of the components referenced in Section 6.1.

X-Road - An open-source data exchange layer, originally developed by Estonia, that enables secure, distributed data exchange between organizations. Widely adopted internationally as a reference implementation of an interoperable exchange layer.



United Nations Development Programme

One United Nations Plaza

New York, NY 10017

www.undp.org

© UNDP 2026