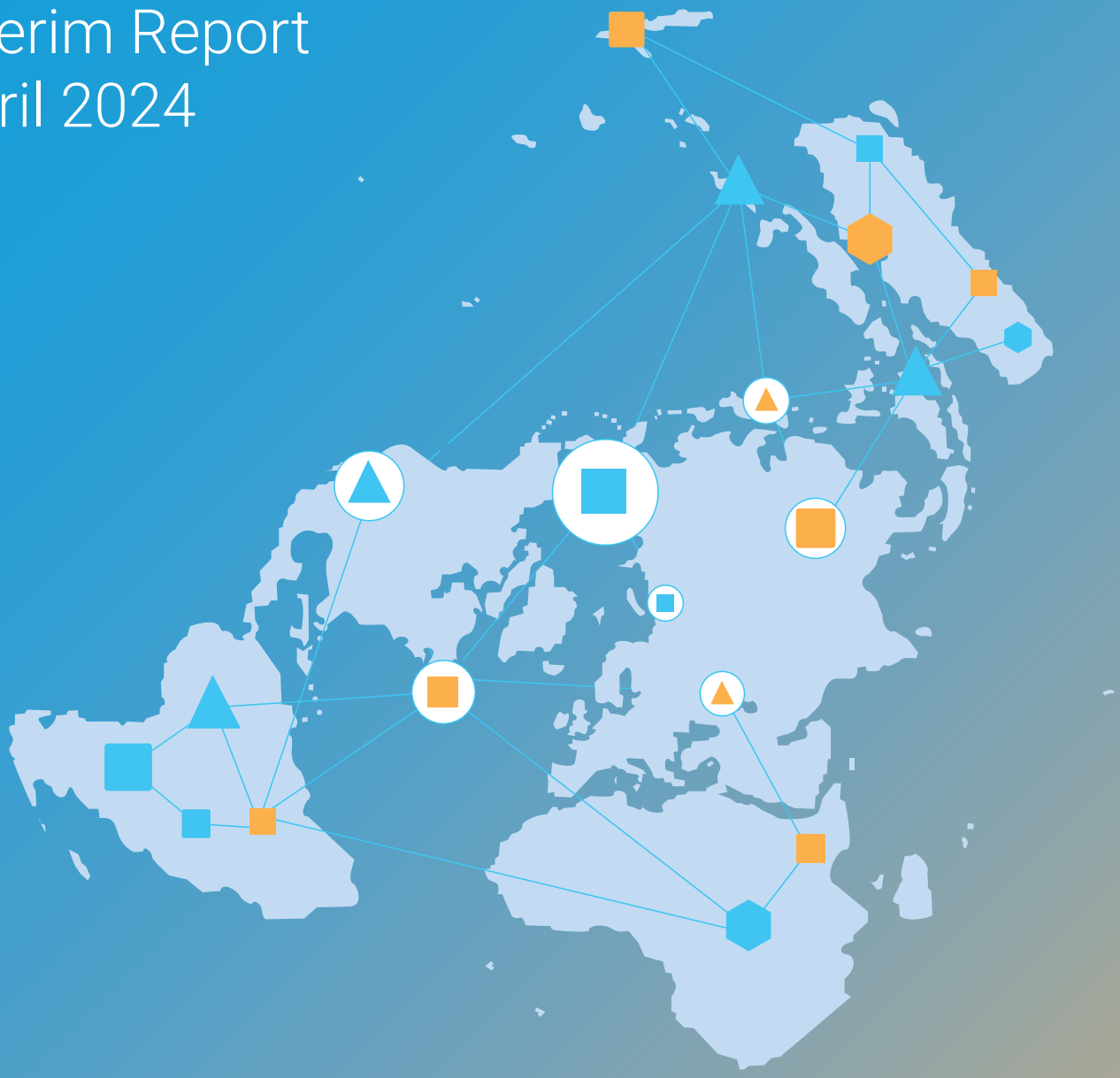
Leveraging DPI for Safe and Inclusive Societies

Interim Report
April 2024



DIGITAL PUBLIC INFRASTRUCTURE
Universal Safeguards

United Nations
Office of the Secretary-General's Envoy on Technology

UNDP

DIGITAL PUBLIC INFRASTRUCTURE
Universal Safeguards

Leveraging DPI for Safe and Inclusive Societies

Interim Report, April 2024

Version 1.0

Office of the United Nations Secretary-General's Envoy on Technology (OSET)
United Nations Development Programme (UNDP)

Table of Contents

Executive Summary

Digital Public Infrastructure (DPI) is made up of secure and interoperable digital systems that enable the delivery of public services. DPI represents a potentially transformative force that can shape societies worldwide, making them safe, stronger and more inclusive. However, if not implemented with care, DPI can cause harm by exacerbating existing inequalities, endangering public welfare, creating new forms of vulnerabilities, and stifling growth.

The multi-phase Universal Safeguards for DPI initiative, launched in 2023 by the Office of the United Nations Secretary-General's Envoy on Technology (OSET) and the United Nations Development Programme (UNDP), sets out to co-create a pragmatic framework for countries seeking to implement DPI, and places safeguard principles, practices, and governance at its core.

This first Interim Report serves as a foundation for gathering multi-stakeholder feedback. The report is derived from an extensive consultative process and presents early findings on the opportunities presented by DPI and notes the urgent need for guardrails. It presents an actionable framework to guide implementation that purposely avoids potential pitfalls. The report also identifies next steps and timelines for developing the Universal Safeguards for DPI.

Section 1.0 About this Interim Report provides suggested forms of engagement and feedback from readers which could be helpful when progressing into the deductive phase and when continuing the co-creation process.

Section 2.0 Introduction establishes trust and equity as key to leveraging DPI for safe and inclusive societies while addressing societal risks that may be created or exacerbated by digital transformation. It highlights the need to embed appropriate measures across all stages of the DPI life cycle and associated governance mechanisms.

Section 3.0 The DPI Opportunity reveals, with provisos, that DPI can act as a potent lever to amplify and enable various existing and emergent pathways of inclusive and sustainable growth and that it can accelerate progress towards achieving the Sustainable Development Goals (SDGs) and be employed to nurture safe and more inclusive societies.

Section 4.0 Urgent Need for Guardrails draws on existing DPI implementations to classify risks, posing them in relation to the stages of the ever-evolving DPI life cycle (scoping; strategy and design; development; deployment and transformation; operations and maintenance); and their origin: technical, organizational or normative (i.e. legal, ethical, regulatory). This section provides a frame of reference to identify, mitigate and manage potential risks and harms associated with DPI implementation and proliferation.

Section 5.0 Actionable framework provides principles- and outcomes-based approaches for implementing in-country and DPI-specific mechanisms. It offers guidance for systematic operationalization of the principles that underpin risk identification, mitigation and management, by all stakeholders across the DPI life cycle. The section also elaborates on the importance of participatory processes and sustained governance across the entire DPI life cycle (including potential interoperability with other systems and DPI) and identifies key governance stakeholders, models and implementations.

Sections 6.0 Next Steps is forward-looking and outlines the subsequent phases of the Universal Safeguards for DPI initiative. The next phase, the deductive phase, showcases how to create the framework on a solid foundation whilst remaining flexible enough to ensure in-country DPI implementation promotes growth and leads to safe and more inclusive societies.

1.0 About this Interim Report

Purpose of this Report

This Interim Report is compiled based on extensive research conducted by 44 experts and practitioners in the field of Digital Public Infrastructure and associated transformations. Given the exhaustive research conducted by the Working Group members, including inputs from the initiative's International Organizations Consultative Group (IOCG), it is extremely difficult to do justice in expression and summarization. This report is a collaborative effort of Working Group members working in their individual capacity and does not imply institutional endorsements of their respective organizations nor is it presented as their consensus.

This Interim Report has been created as a window into the body of work essential for leveraging DPIs for a safe and inclusive society. Through this window, the readers can get a systematic view into important considerations and provide feedback and suggestions for inclusion of critical and vital topics that could limit the effectiveness of DPIs in ensuring safety and inclusion of all people. Readers are encouraged to read, reflect, and share inputs for refinement.

Structure of this Report

A bias for in-country conceptualization, design, organization, and implementation is at the heart of the structure of this report. It explains the context and then explores the various categories of risks that are pertinent to safety and inclusion aspects of DPI. The risks converge in a set of foundational and operational principles that form the basis for systemic action. These principles are woven into operational processes which culminate in the essential governance mechanisms and appropriate organizational designs. Other sections serve as connections to this core structure. Readers are encouraged to find opportunities to improve ideas of what would make in-county implementation more feasible for their contexts.

Leveraging this Report

When reviewing this report, it is recommended to read from beginning to end, identify vital omissions or inconsistencies, suggest supporting evidence and facts, and highlight any parts needing clearer expression. This approach would help improve the second Interim Report, which is due at the next stage of the process when the Working Groups enter the deductive phase.

How to Contact Us

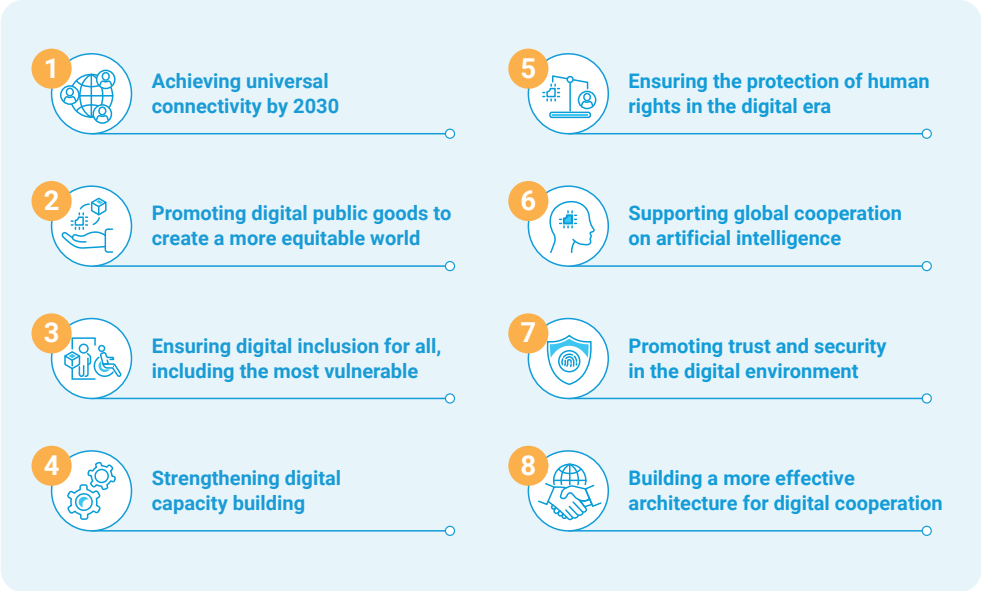
For questions, feedback or clarification, contact: dpi-safeguards@un.org.

2.0 Introduction

Background

The United Nations Roadmap for Digital Cooperation as set out by the United Nations Secretary-General was developed in response to the growing significance of digital technologies in everyday life and their potential impact on future societal developments. The roadmap was an invitation to all stakeholders to actively engage in advancing a safe and more equitable digital world. The key priorities of digital cooperation are enumerated below:

Key Priorities of Digital Cooperation



The United Nations Roadmap for Digital Cooperation was released in 2020. Since then, there has been increasing recognition among countries that DPI, made up of foundational digital building blocks, is important for managing an accountable and responsible interplay of services, resources and information, without causing harm. Under some designs, digital identity, payments and data exchange systems are commonly understood to be the foundational components of DPI. However, other designs are also possible. The concept of DPI is extensive and evolving, with building blocks emerging in other domains such as climate action and healthcare, as well as the fast-moving field of Artificial

Intelligence (AI). If properly designed, organized and governed, DPI can form the backbone of rapidly digitizing societies, facilitating everything from e-services to financial transactions, and can be key to advancing digital transformation across different sectors.

Key Objectives

Trust and equity are key to how DPI can be leveraged to build a safe and inclusive society. Given the fundamental role DPI can play in delivering public services, it is essential that these services benefit all people in a safe and equitable manner, while ensuring that no rights or privileges are degraded or retrogressive measures adopted. To uphold this, the proper actions needed to build a safe and inclusive society should be embedded across all stages of the DPI life cycle, and integrated into all associated legal and regulatory frameworks and governance mechanisms.

Safety underwrites trust

Trust is the cornerstone of institutional legitimacy and societal confidence. It is essential for widespread acceptance and effective implementation of DPI, as well as for the multi-stakeholder participation that unlocks the full potential of DPI. The trust-building process needs to be more than incidental; it should be a deliberate and an integral part of DPI design, regulation, governance, and implementation. This ensures that people's rights are upheld and they receive fair and equitable treatment when interacting with digital services and systems.

Safety is a multi-dimensional concept that underwrites trust. It manifests across all aspects of DPI, for instance through safety-oriented technical measures such as end-to-end encryption of the data that travel through the operational life cycle of a DPI. Other safety-related measures include addressing organizational vulnerabilities, such as through cybersecurity and data governance policies that pertain to access, controls, and the responsibilities of data custodians. However, safety — and by extension trust — are not limited to technology implementation but also depend on stakeholders' perception and experience with the system.

DPI must not only be safe, but must also be seen to be, and experienced as safe, with recourse to responsive corrective mechanisms if it is not. Normative architecture such as legal and policy provisions for transparency, grievance

redressal, as well as for robust human rights due diligence and privacy impact assessments, can enhance safety and predictability. These provisions also strengthen public trust in DPI by offering effective mitigation for risks. People's ability to take part in shaping the concept, design and governance of DPI also boosts trust in the system.

Inclusion as a catalyst for equity

Equity has multiple facets. It implies fair and inclusive access to DPI. The aim is not just to make technology available to everyone; it is about tailoring it to be scalable (up or down) and people-friendly, so that engaging with DPI becomes a seamless experience for all, irrespective of background or resources. Equity underpins all Sustainable Development Goals (SDGs), hence a focus on equity through the DPI life cycle can accelerate achievement of the SDGs. Ultimately, this means ensuring that the disadvantaged and the most vulnerable people can reap the benefits of inclusive and sustainable development.

Inclusivity is essential for fostering equity. It can manifest through design choices that solve problems related to identification or biometric failure, for instance. Similarly, inclusivity should be woven into policies that mandate bias-assessment in service or product delivery. Inclusivity can also be used to incentivize awareness and digital literacy outreach. For marginalized individuals and communities who rely on a government safety net for basic necessities, the consequences of exclusion can be particularly severe and exacerbate existing inequalities. Inclusive DPI design depends on consultations and meaningful engagement with diverse stakeholders during the strategy and design process. This can ensure that the system reflects the concerns and needs of such communities and incorporates iterative improvements that respond to their feedback and grievances.

The DPI Safeguards Initiative

The DPI Safeguards initiative is stewarded by the Office of the United Nations Secretary-General's Envoy on Technology (OSET) and the United Nations Development Programme (UNDP). It aims to leverage DPI to build a safe and inclusive society. Multi-stakeholder Working Group members were thoughtfully selected and announced, volunteering their time and experience to create

universal and unifying safeguards. The safeguards aim to include and protect everyone everywhere and also have a focus on climate protection, safeguarding the planet and accelerating the achievement of SDGs. The initiative is designed to consolidate and expand upon work already carried out in this critical area and leverages the expertise of specialists and institutions worldwide.

The DPI Safeguards Initiative focuses on three key areas:

1. **Develop a DPI Safeguards framework**: From principles to implementation, through multi-stakeholder convenings and expert-led discussions, the framework will focus on principles, processes, and practices, with an implementation lens.
2. **Establish a DPI Safeguards resource hub**: A community hub for the DPI Safeguards initiative, providing updated knowledge, guidance, and resources from diverse partners, as well as facilitating international and in-country collaboration and knowledge-sharing.
3. **Implement the DPI Safeguards framework**: "Lighthouse" implementation in select countries will help apply, learn and improve the DPI Safeguards framework to specific use cases and help devise in-country partnerships for global implementation and scale.

This strategic focus will provide an environment in which DPI implementation is not only secure and inclusive but also practical and adaptable to diverse needs.

A Note on Methodology

The inductive phase of the DPI Safeguards initiative involved intense participation from six diverse global Working Groups. Each group was dedicated to one of six key focus areas under risks (technical, organizational, and normative) and mitigation (principles, operationalization, and governance) with continuous cross-validation amongst them. The Working Groups use a multi-phase approach that incorporates both inductive and deductive reasoning.

During the inductive phase, each group systematically mapped existing definitions and best practices related to DPI safety and inclusivity within their specific area of focus. This phase involved conducting comprehensive reviews and soliciting feedback from a broad spectrum of experiences. The objective was to gain an understanding of the current landscape, study effective practices, and gather valuable insights from real-world DPI implementations. This Interim Report represents the output of the inductive phase, which aims to solicit further insights and experiences from practitioners. Further details about the methodology are available in Annex 6 of this report or in the DPI Safeguards Workbook.

3.0 The DPI Opportunity

Over the last decade, the Digital Public Infrastructure approach has emerged steadily as a demonstrated pathway to accelerate economic progress by purposefully leveraging digital technologies to unlock new growth opportunities while simultaneously tackling our prevailing large, complex and dynamic societal development challenges.

- **Accelerating progress towards SDGs**
- **Enabling inclusive economic growth**
- **Nurturing safe and inclusive societies**
- **Assuring in-country implementation**

Accelerating Progress Towards the SDGs

DPI plays a pivotal role in advancing all the interconnected Sustainable Development Goals (SDGs) by employing digital technologies to address global challenges at scale. Exponential progress is needed to achieve the SDGs by 2030, which may not be feasible without the acceleration afforded by DPI thinking and the multiplication of digital innovations across development sectors. For example, DPI systems such as electronic registries, credentialing systems, digital payment infrastructure, health information systems, and educational and government service platforms have the potential to accelerate financial inclusion; enhance the delivery and quality of healthcare and education; enable climate resiliency and facilitate smart city initiatives, thereby contributing to poverty reduction, hunger eradication, improved health outcomes, quality education, gender equity, and sustainable economic growth.

Enabling Inclusive Economic Growth

DPI designed and implemented to serve public interest at population scale may offer transformative opportunities to accelerate inclusive economic growth by enhancing the efficiency of public services and reducing market coordination costs. The reduced cost of transactions - such as cost of digital Know Your Customers (eKYC), digital signatures or consent based data exchanges - may translate into higher productivity and inclusive innovations. Through streamlined processes and improved access to digital infrastructure, DPI may enable micro-entrepreneurs and underserved populations to access new opportunities and markets. DPI-enabled transactions may produce significant efficiency gains and direct income, contributing to broader economic empowerment and prosperity. The full potential of DPI recognizes its interconnectedness with human rights, ensuring that risks are mitigated, and progress is safeguarded, equitable, and leaves no one behind.

Nurturing Safe and Inclusive Societies

Every endeavour towards sustainable development should ensure that our societies are safe and inclusive. DPI, if designed and implemented with proper safeguards and in a responsible manner, may present a potent opportunity to advance safety and inclusivity across various dimensions. For example, integrated DPI systems may enable real-time communication and coordination during crises, while advancements in healthcare technology may improve patient safety and access to quality care for all, including marginalized communities. DPI may facilitate smart transportation systems to enhance road safety and accessibility, ensuring that transportation services are inclusive and available to everyone. Moreover, DPI may be employed to strengthen cybersecurity measures to protect against digital threats, ensuring the safety and privacy of all individuals, including vulnerable populations. By prioritizing safety and inclusiveness across these domains, DPI has the potential to contribute to the creation of safe, more resilient, and inclusive societies for all.

Assuring In-Country Implementation

The potential benefit of DPI-accelerated opportunities hinges upon effective and sustained in-country execution. Recognizing that implementation occurs within the unique context of each country and its environment, it is imperative to tailor strategies and actions to address local societal needs and challenges. For this reason, it is critical that DPI implementation prioritizes engagement with key stakeholders within the country, including government agencies, civil society organizations, private sector organizations and local communities. As no country operates in isolation, international collaboration and interoperability enabled by DPI plays a pivotal role in realizing economic benefits. By fostering collaboration and understanding the specific requirements and priorities of in-country stakeholders, DPI initiatives can maximize their effectiveness and relevance, ultimately realizing the opportunity to leverage DPI for safe and inclusive societies.

The benefit of DPI opportunities also hinges on design and implementation that mitigates any unintended consequences, particularly impacting vulnerable and marginalized populations. By proactively addressing potential risks, it is possible to navigate the complexities of DPI acceleration while fostering safe, inclusive and sustainable outcomes for all.

4.0 An Urgent Need for Guardrails

Although DPI has the potential to enable inclusive economic growth and accelerate progress towards SDGs, DPI still poses several risks that may impede progress or cause harm. Improperly or inappropriately designed and implemented DPI may result in risks at all scales of social organization: individual, community (geographical, social etc.), institutional, regional, national and global. Risks to individuals and communities differ according to factors that include, but are not limited to race, ethnicity, gender and disabilities. Some risks are national and impact economies and national security; others are regional, global or geopolitical and impact international relations, regional and global markets, and more. Several risks impact multiple scales simultaneously, for example at community and national scale or at global and environmental scale.

4.1 Risk Cases Observed

Risks observed in DPI deployments present a valuable opportunity to learn from and inform the design and implementation of guardrails for future implementations. These guardrails are necessary to ensure that DPI is safe, and also that it is leveraged for safe and inclusive societies. For this purpose, it is useful to consider risks that expose people to human rights violations; and those that unnecessarily limit the possibilities for growth, such as distortions in the market.

1. Human Rights Violations

The Universal Declaration of Human Rights (UDHR) establishes a common standard of rights for all. These include civil, political, economic, social, and cultural rights. Improperly designed and implemented DPI systems, including the associated governance mechanisms, have been found to present risks of human rights violations including discrimination, exclusion, interference with privacy, and limited or no access to justice and the rule of law.

Discrimination: The UDHR ascribes to all persons various rights and freedoms without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth, or other status. DPI may provide opportunities for intentional and unintentional discrimination based on these or other characteristics, such as ethnicity, caste, socio-economic status, immigration or refugee status. These are prominent grounds of discrimination in access to identity (ID) documentation, especially proof of nationality, as 75 per cent of the world's stateless are from national, racial or ethnic minority groups.

Personal data collected by national digital identity systems and other DPI systems may be used to discriminate against minority and historically marginalized communities. They may also be used to target particular ethnic, religious or other minorities, as well as to repress political dissidents and human rights defenders, or to surveil or block political opponents. Furthermore, the incorporation of AI into DPI solutions could increase the risk of discrimination when determining eligibility for health, financial, educational and other DPI services.

The submission of personal data may force mischaracterization, for example when gender non-conforming individuals are required to identify as either male or female. Discrimination can contribute to exclusion by limiting opportunities for marginalized groups.

Exclusion: Human rights are violated when people cannot access essential or critical services. This has been observed with national digital ID cards and other mandatory enrollment systems. Where no alternative means of access is available, exclusion may result from prevailing digital divides, poor system design, arbitrary or discriminatory policies and practices, and a variety of other reasons. Persons with disabilities (PwDs), for example, risk exclusion when DPI user interfaces do not cater to their particular needs and when they are unable to provide usable biometrics where required. Individuals may face exclusion where their proxies (such as legal guardians and other stewards) cannot interact with a DPI on their behalf. The absence of alternative forms of identification for those unable to access the digital interfaces of DPI has been the grounds for litigation.

When an individual is not considered to be a national or is denied proof of nationality by competent authorities, they face heightened risk of exclusion from DPI systems, which can amplify their marginalization and shut off their access to basic necessities like employment, food subsidies, or emergency healthcare. Persons in humanitarian settings (displacement, refugees and asylum seekers), may face increased risk of statelessness.

Interference with privacy: Human rights are violated when there is arbitrary interference with an individual's privacy. Risks arise when personal information is shared without an individual's consent, and when revocability of consent is difficult, including when full records of transactions are not available to the individual. DPI systems which provide access to sensitive health data, for example related to birth or abortion, could present privacy risks, particularly for women and girls.

In multiple cases, the mandatory collection of biometric data has been ruled unconstitutional and a violation of human rights and civil liberties, including the right to privacy. Even without mandatory collection, centralized storage of biometric information (e.g. fingerprints, iris scans, facial geometry) in large scale DPI systems can introduce risks since such data is non-fungible in case of data breaches and could be abused.

Risks are amplified when DPI systems are poorly designed and when data is shared across interconnected systems. In ubiquitous DPI systems which interconnect various services and span many areas of everyday life, the behaviour of large portions of the population is observable, enabling public and private sector agencies to track individuals. Indeed, research shows a rise of digital surveillance systems on the back of national biometric registries.

Access to justice and rule of law: Human rights are violated when persons are unable to seek remedies for acts violating the fundamental rights granted by the constitution or by law. Absence of grievance and redress mechanisms in DPI may constitute a human rights violation. As evidence from some countries shows, hesitancy among vulnerable communities to use technological grievance redress systems due to distrust in capacity limitations or other factors, may heighten the risk of exclusion from such channels.

The absence of independent judicial oversight jeopardizes the protection of human rights for those who have been excluded from accessing and benefiting from DPI. In at least one case, a lawsuit has been filed for the absence of adequate regulatory oversight which enabled harms such as unlawful and unconsented financial deductions, vulnerability of personal data, and predatory practices in a DPI. Case law calling for judicial oversight of specific DPI systems sheds light on just how crucial oversight is to DPI, and offers critical guidance to ensure that safeguards are in place to reduce exclusionary risks.

2. Market Distortions

Concentration of market power among a few actors may cause harm from and limit the benefits of DPI, for example by limiting sovereignty, services, and consumer protection. The harms of market distortion are most felt in the absence of protection mechanisms. These include but are not limited to the rights of individuals and whistleblowers to raise concerns about unfair practices, as has been cast into law in some jurisdictions.

Sovereignty: Among other consequences, the concentration of market power can impede sovereignty in areas such as data, technology, cyber, and intellectual property (IP). Data sovereignty involves determining how data is generated within a country's jurisdiction, and how it is collected, stored, processed, and accessed, including the ability to enforce regulations regarding data protection, privacy, and security. Without such authority, DPI may be more prone to the violation of human rights and affect other harms. Some DPI systems, though nationally provisioned, have cross-border implications, and this gives rise to risks such as impeding cross-border data flows, vulnerabilities of data capture, and geopolitical dependencies.

Technological sovereignty concerns the capacity to develop, own, and control critical digital technologies, systems, and infrastructure, reducing dependence on foreign technology providers and ensuring autonomy in decision-making related to digital innovation and development. Dependencies on large foreign technological companies for cloud services is a typical case of concern. Several other risks have been observed, including vendor lock-in, high service delivery and use costs, and interoperability challenges. This is accompanied by supply chain risks that might be affected by geopolitics, which in turn may limit

countries' flexibility to adapt to new technologies or eliminate incentives for local development. In sum, these dependencies put DPI at risk of violating a variety of human rights and causing other harms. The reliance on profitable service delivery businesses to be built on top of DPI infrastructure without adequate safeguards is a risk to the value, adoption, and sustainability of the DPI itself.

Cybersovereignty concerns the ability to protect national interests and security in cyberspace, including the authority to establish and enforce regulations, policies, and norms governing online behaviour, cybersecurity, and digital rights within national borders. Such vulnerabilities give rise to various risks to DPI host countries, including increasing their cyber attack surface towards adversaries.

Intellectual Property (IP) sovereignty concerns the authority to govern the creation, use, and protection of IP within a nation's jurisdiction, encompassing the ability to enact and enforce laws and regulations pertaining to patents, copyrights, trademarks, and trade secrets. There are cases in which the patents for DPI technology are held by their private owners, and this increases dependence on a private sector entity. Among other things, such IP ownership restrictions limit the manner and extent to which innovation can be used to reduce harms, improve adoption by the marginalized and ensure that the benefits of DPI are reaped by all.

Services: Not only the breadth of service offering, but also the nature of the offerings are significant determinants of whether human rights are violated, and other harms are generated through the use of, or lack of access to, DPI. Where there is monopoly control over a DPI, with significant barriers to entry, there is a risk that innovation is stifled and demands of the market for appropriate products, services and features are unmet.

Consumer protection: Market dominance generally results in anti-competitive practices such as price-fixing or collusion. Concentration of market power has been seen in some national digital payments systems and measures like caps on market share have been used to protect the interest of consumers and maintain a competitive landscape.

Risk Categories

DPI systems comprise standards (including protocols), technological systems and services that operate at the intersection of individuals, on the one hand, and public and private entities that hold institutionalized political and economic power, on the other. Risks therefore derive from failures and inadequacies in the overarching legal, regulatory and ethical (normative) frameworks in which they operate, encompassing all organizations and stakeholders that have a role related to DPI service delivery. Risks also lie within the technological systems themselves.

Risk Categories

- Normative risks
- Organisational risks
- Technical risks

1. Normative Risks

The vibrant community of innovators, service providers and other actors, characteristic of an ideal DPI, is accompanied by diluted accountability through distributed and fragmented responsibility, potentially giving rise to a variety of risks. The absence of deliberate, purposeful and effective normative frameworks may leave human rights and market distortion risks unmitigated.

Human Rights Risks: Normative risks arise in the absence of an overarching framework which prescribes relevant legal, regulatory and ethical requirements to mitigate human rights violations. For example:

- **Discrimination** may occur in the absence of requirements for human rights impact assessment and privacy-by-design of DPI; as well as non-discriminatory, voluntary and unconditional use of DPI
- **Exclusion** may occur in the absence of requirements for human rights impact assessment and privacy-by-design of DPI, as well as non-discriminatory, voluntary and unconditional use of DPI

- **Interference with privacy** may occur in the absence of requirements for human rights impact assessment and privacy-by-design of DPI; as well as voluntary and unconditional use of DPI
- **Access to justice and rule of law** may get compromised in the absence of privacy-by- design, non-discriminatory use, voluntary and unconditional use, human rights impact assessment, and in-built governance mechanisms

Market distortion risks: As the observed DPI risks reveal, there are a number of harms that may arise from market distortion, in particular limitations on sovereignty, services and consumer protection. Normative risks arise in the absence of an overarching framework which prescribes relevant legal, regulatory and ethical requirements for example:

- **IP sovereignty and innovation are hampered** in the absence of requirements for the use of open and interoperable standards; research, monitoring and evaluation programmes; and the application of privacy-by-design. These in turn may constrain the scope and features of services, leading to human rights and other harms.
- Many **risks associated with monopolies** may arise in the absence of requirements for the use of open and interoperable standards, and in-built governance mechanisms.
- **Risks of AI-based discrimination** may arise in the absence of requirements for privacy-by-design, non-discriminatory use; research, monitoring and evaluation, and in-built governance mechanisms.
- **Environmental risks** may arise in the absence of requirements for privacy-by-design, human rights impact assessment, open and interoperable standards; and research, monitoring and evaluation.
- **Geopolitical risks** may arise in the absence of requirements for privacy-by-design, open and interoperable standards, and in-built governance mechanisms.
- **The risk of system failures** may arise in the absence of requirements for research, monitoring and evaluation; open and interoperable standards, and in-built governance mechanisms.
- **Technology design risks** may arise in the absence of requirements for open and interoperable standards, and in-built governance mechanisms.

2. Organizational Risks

A DPI ecosystem comprises of diverse stakeholders. They include public sector organizations, planners, legislators, regulators, and adjudicators, private sector providers of software, cybersecurity, cloud services, and data analytics, maintainers of infrastructure, international and national standards bodies, international organizations (e.g. World Bank, UNDP, ITU, OHCHR), individuals, funders, non-profit organizations, community representatives and a variety of other actors. Together, the policies and practices of organizations, institutions, standards bodies, and international organizations comprise the "organizational framework" for DPI.

The organizational risks of a DPI arise from the framework design as well as its implementation in practice, regardless of design. These failures are particularly apparent in the way different stakeholders engage within the DPI, as well as the manner in which their policies, procedures and practices interact with, shape, and are shaped by DPI. The risks arising from organizational failure impact all levels of social organization: individuals, communities, institutions, countries, regions and the world.

Individual and community risks: Organizational shortcomings that contribute to human rights violations include the absence of policies and practices (including robust enforcement mechanisms) that are inclusive, and that protect the rights and interests of marginalized and under-represented constituencies. The lack of diversity within organizations, inadequate representation of impacted individuals and communities at all stages of the DPI life cycle (on the part of the process or the capacity of representatives to participate), and failure of the organizational framework to consider rights and interests of those impacted throughout the life cycle, also contribute to risks. The failure to appropriately design for and manage engagement with specific communities e.g., indigenous communities, refugees, displaced or stateless people, gives rise to several risks. Weaknesses in institutional policies and oversight have multiple impacts, including the possibility of privacy and data protection breaches as well as discrimination on account of the absence of data sovereignty. The absence of proper accountability and remedial measures, along with institutions to manage them, all undermine trust in DPI.

Institutional risks: Risks arise when institutions (including public organizations and private service providers) responsible for building or maintaining DPI systems are not subject to meaningful transparency and accountability mechanisms. This can lead to several harms, including privacy violations, fraud, technical failures, and lack of accountability. Additionally, risks stem from the absence of appropriate institutions to oversee the entire DPI life cycle or the absence of institutional mechanisms and capacity to fulfill assigned roles in the life cycle. Poor coordination among key institutions and failure to contextualize institutional needs for specific contexts may also jeopardize the safety of DPI.

Country-level risks: Organizational failures that contribute to national-level risks include lack of will or wherewithal to coordinate (and where necessary cooperate) between key agencies and stakeholders in the ecosystem, to employ a whole-of-society approach to DPI, and to conduct public consultations. Insufficient organizational enforcement and oversight measures that lead to data leaks pose national-level risks, as does undue reliance on political and geopolitical dynamics.

Regional and global risks: Institutional voids may lead to poor cross-border cooperation on DPI and, as a consequence, a lack of standardization across different systems. This impedes the delivery of seamless digital services globally. At the same time, strategic alliances based on shared DPI technologies and standards may lead to geopolitical consequences including the emergence of digital blocs, which may impact international relations and trade.

3. Technical Risks

Technical implementation of DPI is crucial for its adoption and sustainability. The technical dimension plays the vital role of enabling services and laying the foundations for trust, reliability, inclusion, data privacy and security, protection from fraud, equitable access and other features that mitigate risk, such as human rights violations and market distortions. Technical risks impact individuals and communities, countries, regions, and the world, with many intersecting factors.

Individual and community risks: Risks that predominantly impact people and communities occur when the DPI is not designed to mitigate human rights violations or implemented to match the design and iteratively tested with intended individuals and communities. Risks to people and communities also

occur when services are not delivered to, and accessible by, individuals; and when they have no recourse mechanisms for complaints regarding security and privacy breaches.

Country-level risks: Technical risks that have country-level impact arise from technology choices that prevent interoperability, scalability, sustainability, sovereignty and ownership of the DPI. These risks also arise from an inadequate focus on mitigating the risk profile of the country, and on resilience, reliability, availability, scalability, and quality of service; inadequate skills and capital to develop domestic DPI in line with global standards, and inadequate focus on various forms of fraud. Risks arise from security vulnerabilities introduced when the DPI is implemented, for example that derive from the complexity of supply chains and siloed accountability. Siloed implementation also leads to lack of interoperability, a major technical risk. Other country risks arise from cost overruns, unforeseen external influences and various factors that cause delays. Major technical risks may emerge when DPI systems are not adequately maintained, improved and updated, as this gives rise to new threats.

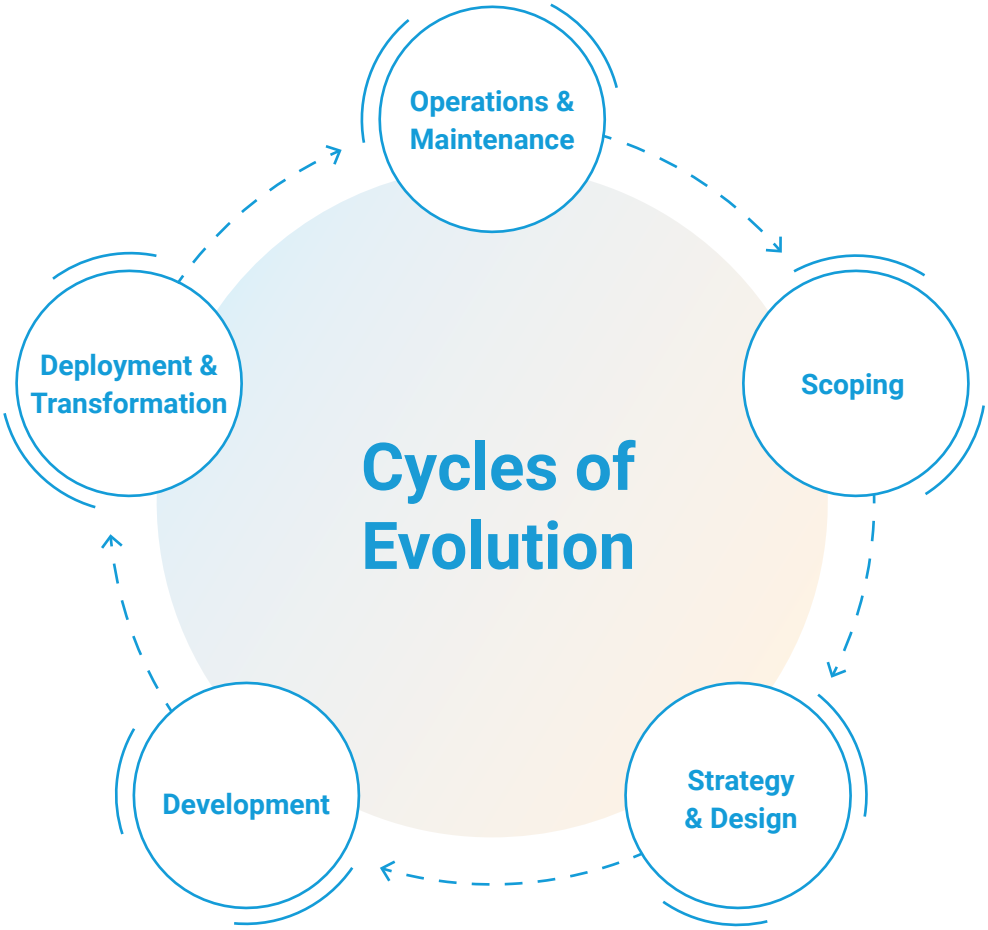
The deployment of DPI systems could have harmful effects on the environment, including excessive energy consumption or exacerbating water scarcity. This is the natural consequence of using massive, population-scale information technology systems. Such systems require large data centres with significant IT infrastructure, which call for high energy and water consumption. This is a rapidly growing concern with the scaling of DPI.

Regional and global risks: Technical risks that have regional or global impact occur when global open standards, including those governing cybersecurity, interoperability, usability, diversity and universality, are not employed. Such standards are fundamental to seamless interaction between different DPI systems and individuals' ease of access, as well as to global communication and collaboration to facilitate international trade and exchange. They are also essential for scalability and integration with legacy systems. Risks associated with the use of proprietary software include vendor "lock-in" with its associated potential harms at all levels of social organization, as discussed previously.

Other risks include resource wastage, and inefficiency from unnecessary duplication of effort. Poor rollout in one country may diminish enthusiasm by others, and there is a risk that public trust in regional organizations involved in the DPI is eroded.

4.2 Risks and DPI Life Cycle

Just like any large and complex societal transformation, a country adopts DPI over a life cycle composed of stages and activities. While these are nuanced, based on the social, political, economic, environmental or technological ecosystem of each country, a DPI life cycle generally comprises the following stages: scoping, strategy and design, development, deployment and transformation, operations and maintenance, as depicted below.



This nominal DPI life cycle is included as a useful scaffolding to develop a generic framework of risk identification, mitigation and management through processes, operationalization and governance mechanisms across this initiative. DPI implementations may continue to evolve, with adjustments to all, or some stages of the life cycle, as necessary. This ensures relevance and value in the context of a country or DPI.

What follows are nominal activities that fall within different life cycle stages, and their evolution. Actual implementation may employ all or a subset of activities, depending on various contextual factors including, but not limited to, implementation maturity. Technical, organizational and normative risks variously apply to each stage of the life cycle: many singularly, some in multiple stages and others spanning all the stages. Sector- and product- specific risks should be identified, in-context, during specific DPI implementations.

Scoping

The scoping stage of the DPI life cycle is crucial as it establishes the purpose, goals, constraints, and boundaries of a DPI. This then guides subsequent decision-making and ensures alignment with strategic and operational objectives as well as people's needs. Nominal activities include:

- clear framing of the goal or problem
- identifying root societal needs
- targeting core service delivery gaps
- assessing impact potential
- analysing the enabling environment for barriers to DPI implementation, effectiveness and adoption, including existing policy, legal and regulatory frameworks
- taking into account the relevant technical, organizational and normative risks to safety and inclusion

Poorly scoped DPI implementation can result in resource wastage, frustration and aversion. This is particularly so as DPI may not suit all sectors and contexts for a variety of reasons, including legacy barriers to data-sharing across institutions; competition issues; unequal digital readiness across the ecosystem; potential harms or risks at a population scale; or capacity shortfalls. Experience has shown that flourishing DPI systems have generally benefited from extensive support for national rollout, coupled with a robust regulatory regime with effective compliance mechanisms. Others have floundered, on account of under-resourcing and a variety of contextual challenges.

Strategy and Design

This stage of the DPI life cycle is critical. This is where a comprehensive plan is formulated and the DPI design is conceptualized in order to translate objectives into actionable steps that meet functional and performance objectives. This stage includes activities such as mapping and engaging with stakeholders to understand individual needs, identifying parties for collaboration, and advocating for the removal of barriers to DPI implementation in the enabling environment. It also includes planning for optimum service delivery, learning from successful DPI models and best practices. This includes setting design objectives including scalability and sustainability where applicable, with a focus on small, incremental improvements, resilient architecture, and future-proofing the infrastructure. Also, this stage involves establishing standards and protocols and performance metrics to assess adoption and societal impact, preparing design specification according to inclusive and other critical design principles and mitigating design-related technical, organizational and normative risks.

Development

In the development stage, a prototype DPI is built according to defined specifications, ensuring functionality, reliability, and scalability. Activities include software coding to design specification; testing; building open APIs and sandboxes to empower developers (as appropriate to the maturity of DPI implementation and the local context); creating Minimal Viable Products ("MVPs") and running pilot projects to iteratively adjust. Any adjustments should be guided by insights into practicality and impact, while identifying and mitigating risks related to security, privacy, and user experience. This phase ensures that DPI solutions are thoroughly tested and refined before widespread implementation, to minimize risks and maximize effectiveness. Development includes the framing of outstanding policies and regulations, where necessary, and establishing institutional structures in parallel with the technology. Mitigating technical, organizational and normative risks associated with implementation is critical in this stage. A robust governance framework should be put in place.

Deployment and Transformation

During the deployment and transformation stage, the DPI is implemented in its operational environment, and any necessary organizational changes are

made to maximize its impact and adoption. Implementing DPI in its target environment entails installing, configuring, and activating the hardware, software, and networking components in a phased manner; scaling if necessary and appropriate; refining on the basis of evidence and data of users' feedback (and using change management strategies); regularly engaging with stakeholders and communicating widely to ensure successful large-scale adoption so that the benefits of DPI are fully realized across all sectors of society. It is essential that, in parallel, a robust governance framework including monitoring and redressal mechanisms, is activated.

Operations and Maintenance

Once DPI is commissioned, it is expected that individuals regularly interact with its services, and that government agencies rely on its systems for their operations. Regular operations and maintenance ensure ongoing optimal performance, stability, and efficiency of the DPI within the operational environment. Nominal activities include:

- continuous management and maintenance that ensure performance metrics are met, with oversight and accountability
- continuous testing of safeguards to ensure privacy, security, usability, and inclusion
- monitoring, learning and continuously improving alongside innovative methods for engagement, monitoring and evaluating effectiveness, and strategic preparedness for swift action in response to policy windows or opportunities for scale-up
- reviewing technical, organizational and normative risks and mitigation strategies
- ongoing review of governance and assurance that inclusive redressal mechanisms are fit for purpose

Cycles of Evolution

There is a need for constant reflection on, and refinement of, the overall system enabled by DPI. Given the dynamic nature of the field, this should be cyclical and iterative, with re-scoping if and when required. A shift into the strategy and design phase can be done when a substantial change is deemed necessary. The journey of the DPI progresses through a roadmap, introducing capabilities in layers while continually ensuring safety and inclusion. This process evolves as more impactful and inclusive use cases emerge, or when new or unanticipated

risks are identified. This process ensures the DPI continues to serve the public interest effectively and securely and that evolution and effectiveness of governance keeps pace with the adoption across the society.

4.3 Key Takeaways

Given the pace of change induced by the adoption of DPI, the need for safety and inclusion guardrails is becoming even more urgent. Digital technologies have historically demonstrated exponential adoption. The risk of guardrails lagging behind the speed of DPI proliferation is real.

Guardrails are important, not only to ensure that DPI is safe and inclusive but also to leverage DPI to build societies that are safe and inclusive for all persons on our planet. Guardrails are also essential for sustained economic development. The implementation of such guardrails calls for considerable planning and execution. Guardrails should take into account the risks associated with each stage of the iterative DPI life cycle, from scoping to evolution, and be underpinned by trust and multi-stakeholder responsiveness.

Effective guardrails requires an understanding of the different risk categories: technical, organizational and normative; as well as the scale of potential harms: individual, community, institutional, national, regional and global. Unbundling risks in this manner forms the basis for conceptualizing and articulating practical mitigation strategies. These strategies are associated with different stages in the DPI life cycle, some of which are cross-cutting. This approach is crucial for navigating the complexity of operationalizing and governing change within context.

5.0 Actionable Framework

5.1 Mitigating and Managing Risks

A bias for in-country implementation is at the heart of this initiative. The risk categories identified above need to be mitigated, and residual risks need to be managed proactively in the context of each country and its sociopolitical environment. For this to be effective, a set of principles (foundational and operational) are essential to align systemic action by all stakeholders in a holding environment that creates trust and multi-stakeholder responsiveness during implementation.

The principles need to be woven into operations through processes supported by appropriate capacity across the DPI life cycle. Essential governance and assessment mechanisms need to be instituted for sustained effectiveness of guardrails. This is because DPI operates in complex and dynamic societal ecosystems. The following sections cover the principles, operationalization and governance of DPI.

5.2 Harmonizing Principles

Shared principles improve alignment: Principles are fundamental propositions. They serve as a strategic foundation to build an implementable, universal, evolvable, and representative framework for effective and legitimate functioning of a system. They also form a vocabulary to foster shared understanding of concepts, and to enable sustained cooperation. To mitigate and manage risks around safety and inclusion, it is important for all stakeholders of the DPI ecosystem to align on such a foundation.

A wide variety of research methods were used in this initial scoping process. This included reviewing secondary resources and analysing global case studies, all of which informed the principles highlighted below.

Principles that enable safety and inclusion: Existing discussions and prior literature on DPI coalesce around a common set of technical, governance,

community, and ecosystem-related principles. The objective of this initiative is to highlight key principles that underpin the framework, to mitigate and manage risks, and strengthen our ability to build safe and inclusive societies within an overarching framework that is built on human rights.

Specific factors should be addressed, such as establishing suitability and contextual specificity and being responsive to diverse use cases (such as urban or rural) and sectors (such as health or climate action). Capacity limitations (such as digital literacy) and prioritization of key inclusion aspects (such as gender responsiveness) need to be considered across the DPI life cycle and its analog twin.

Foundational and operational principles: Based on the risks identified above, the following section proposes a set of aligning principles to mitigate and manage their potential impact across levels. 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 which may vary across contexts.

Foundational Principles: DPIs that Foster a Safe and Inclusive Society

- **Do no harm**
- **Do not discriminate**
- **Are not exclusive**
- **Reinforce transparency and accountability**
- **Guard by the rule of law**
- **Promote autonomy and agency**
- **Foster community engagement**
- **Ensure effective remedy and redress**
- **Focus on future sustainability**

Foundational Principles

DPI that fosters a safe and inclusive society…

1. **Do no harm**: Harms to individuals may not be immediately obvious. A human rights-based framework should be integrated throughout the DPI life cycle to proactively and effectively assess and address any potential human rights harms and power differentials.
2. **Do not discriminate**: All individuals, regardless of their intersecting identities, should be empowered with unbiased access. Circumstances of historically vulnerable communities, marginalized groups and those who opt out should be included in every risk assessment.
3. **Are not exclusive**: All individuals should have alternative modes (digital / non-digital) to access services enabled by DPI based on their individual capacity and resources. Modes of access should not be limiting, conditional or mandatory — explicitly or de facto.
4. **Reinforce transparency and accountability**: DPI should be developed with democratic participation, public oversight, promote fair market competition, and avoid vendor lock-in. All partnerships should be transparent, accountable, and publicly governed.
5. **Guard by the rule of law**: DPI should be introduced with a clear legal basis and regulated by laws. Regulatory frameworks should be supported with capacity for sector-specific tailoring (e.g. health), implementation and oversight.
6. **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 ensure their society's well-being.
7. **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 engage, participate at critical junctures and actively provide feedback in an environment of transparency and trust.
8. **Ensure effective remedy and redress**: Complaint response and redress mechanisms, avenues for appeal, supported by robust administrative and judicial monitoring and review processes, should be accessible to all in a transparent and equitable manner.
9. **Focus on future sustainability**: Emphasizing foresight is a key responsibility to anticipate and limit long-term harms. For example, environmental impacts of DPI due to factors such as e-waste management policies of countries should be assessed and addressed.

Operational Principles

DPI that fosters a safe and inclusive society…

1. **Leverage market dynamics**: DPI should foster an increasingly inclusive environment for public and private innovation such that market players compete and introduce diverse solutions that cater to the emerging needs of all participants in society.
2. **Evolve with evidence**: Independent, transparent and continuous assessments (such as human rights due diligence and data protection) should engage with people, review evidence and rapidly cease or initiate activities that contain heightened risks or harms.
3. **Ensure data privacy by design**: DPI should embed technical rules that enforce core privacy principles (e.g. data minimization, provisions to delink, and the ability to limit observability by purpose and time) and governments should enact legal safeguards around them.
4. **Assure data security by design**: DPI should embed security measures such as encryption, to protect personal data. A legal framework should fill the gaps where technical design may not be enough to protect data privacy and security.
5. **Ensure data protection during use**: Personal data should be processed and retained lawfully by authorized personnel within a legal framework including complete transaction history, data subject rights, and protections against overreaching information requests.
6. **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 their access or use. DPI should not exacerbate existing challenges or introduce new barriers and inequalities.
7. **Practice inclusive governance**: Long-term effectiveness of DPI is contingent upon a robust legal, regulatory and institutional framework that promotes transparent and participatory governance focused on safety and inclusion.
8. **Sustain financial viability**: As DPI systems form the basis of a society's infrastructure, they should be accompanied by a sustainable financing model. Governments can take lead in the build phase, and local digital ecosystems or the private sector can participate in operations and maintenance.
9. **Build and share open assets**: DPI should share and reuse open protocols, specifications, Digital Public Goods (DPGs) and other building blocks. This

enhances flexibility and assures that proprietary systems do not limit the ability to improve safety and inclusion.

Operational Principles: DPIs that Foster a Safe and Inclusive Society

1. **Leverage market dynamics**
2. **Evolve with evidence**
3. **Ensure data privacy by design**
4. **Assure data security by design**
5. **Ensure data protection during use**
6. **Respond to gender, ability or age**
7. **Practice inclusive governance**
8. **Sustain financial viability**
9. **Build and share open assets**

Operationalizing the principles: These principles should inform and integrate with various stages of the DPI life cycle and related processes. It is critical to translate these principles into processes and controls, in the absence of which they may remain philosophical statements. The next section outlines how principles translate into actions (i.e. operationalize) to improve safety and inclusion through the various stages of the DPI life cycle.

5.3 Systematic Operationalization

The need for systematic operationalization: Due to the multifaceted nature of DPI thinking, its diverse applications, emerging perspectives of stakeholders and the dynamic nature of DPI ecosystems, it is important to appreciate that the related operational frameworks and processes will continually evolve. Principles that underpin the mitigation and management of risks and build safe and inclusive societies need to be systematically woven into day-to-day operations of all stakeholders engaged in the DPI life cycle.

Successful operationalization is about outcomes, i.e., implementing the principles and avoiding the pitfalls. At its core, this entails taking measures to act on the principles, accelerate field implementation (i.e. operationalization), institutionalize governance and realize the desired outcomes.

However, note that the aspects of operationalization detailed below are derived from analysis carried out during the inductive phase. These aspects will undergo substantial refinement during the deductive phase to ensure their effectiveness during in-country implementation.

Systematic Operationalization

1. **Foundation operations assessment**
2. **Stakeholder capacity-building**
3. **Strengthening operational processes**
4. **Strengthening data protection**
5. **Effective impact assessment**
6. **Redress and access to justice**
7. **Monitoring and evaluation**
8. **Systems approach to maintenance**

1. Foundation Operations Assessment

Operational measures entail practical commitments, such as written laws, regulations and policies, to oversee how DPI functions. This is achieved by employing transparent legal and administrative checks and balances. Operational measures should derive from relevant laws, norms, and standards, including international legal instruments, such as human rights treaties, non-binding international normative guidance, for example, the Sustainable Development Agenda, including related frameworks and standards.

DPI adoption should be non-exclusionary and yet retain optionality, and not be mandatory. Operationalizing requires significant forethought and investments in human-to-human infrastructure and offline systems, as permanent service-

layers and not interim measures, to ensure that systems remain optional throughout the entire DPI life cycle.

Establishing DPI operating processes includes adopting or amending appropriate legislative measures to ensure safe operations and effectively prevent misuse and/or abuse of power. Monitoring and evaluating day-to-day operations is essential for effective implementation and control by diverse stakeholders across public and private sectors.

Instituting mitigation measures related to policies, practices and capacity-building requires significant political will, foresight, planning, competencies and skills, and long-term political and economic commitment. DPI implementers need to consider (through a process that includes robust public participation), the legal, financial, and social initiatives required for these foundational operations before implementing DPI.

2. Stakeholder Capacity-Building

Multi-stakeholder capacity: DPI implementation spans the work of diverse stakeholders, including the government. Capacity-building needs vary across different stakeholder groups. If designed in a transparent, participatory and inclusive manner, DPI-related capacity-building can achieve significant downstream advantages.

Community engagement capacity: Government and industry should appreciate the ability of community-based service providers to engage with people and operationalize DPI in an inclusive manner. These providers ensure that systems address the needs of marginalized groups in society. Regular communication is critical so that upgraded or new services are used, and benefits are derived for themselves and their communities. This is needed from the earliest inception of DPI.

Private sector capacity: The private sector may view DPI with uncertainty due to concerns that the business advantages gained from proprietary technology could be compromised by competition. It is imperative to sensitize, educate and develop their capacity to derive the benefits of DPI. DPI components and derivative systems may be developed by the private sector, local digital ecosystems, and start-ups. Building their capacity is important for safe and inclusive adoption of DPI.

Interagency and interdisciplinary collaboration capacity: Public and private sector DPI administrators should consider incorporating training and capacity-building during their interagency collaborations, including designing core competencies for hiring and developing staff in these areas.

Judicial capacity: Ensuring independence and access to justice are critical components of safeguarding DPI at an operational level. For judicial actors to play an effective role in the implementation of laws, regulatory frameworks, and to oversee operations in practice, they should understand the complex design of DPI. This requires judicial training.

3. Strengthening Operational Process

Rule of law: Operational measures are essential to secure and sustain the rule of law. According to the United Nations, rule of law "is the implementation mechanism for human rights, turning them from a principle into a reality. Where such rights are justiciable or their legal protection is otherwise ensured, the rule of law provides the means of redress when those rights are not upheld, or public resources are misused". In addition to the rule of law, appropriately adapted DPI regulatory frameworks should be developed and implemented.

Access to information laws and policies: In practice, many right-to-information laws are only partially operational. Common exemptions from disclosure under such laws can be invoked in an overinclusive way to prevent members of the public from accessing basic information about the design or implementation of DPI. For DPI to be truly open and public, access to information laws is critical during all stages of the life cycle, including early piloting.

Open procurement: Transparent, competitive, and high-quality procurement practices are fundamental to DPI operationalization. Procurement processes should meet internationally recognized good practices, particularly in terms of transparency and competition. This includes processes to assure availability of in-house technical expertise, vendor qualification, technical or process specifications, documentation and knowledge transfer to support the building of local competencies, and the use of open international standards.

Human rights due diligence: Those engaged in developing and delivering DPI should adopt and comprehensively develop, publish, and implement the human

rights due diligence procedures, processes and practices. This entails thorough risk-mapping, risk evaluation, mitigation, alerts and complaint mechanisms, and monitoring and evaluation systems. Within supply chains, end users and members of the value chain should make transparent commitments to respecting human rights. Companies should publish policies stipulating their human rights expectations regarding operations, services and the use of products.

Transparency for public participation: Public participation here refers to public engagement in legislative, regulatory and operational processes. Many critical elements of operational checks and balances are reserved for regulatory rulemaking, and are not properly referenced or addressed in primary legislation. Regulatory rulemaking can be abstract and inaccessible, particularly for vulnerable and marginalized populations. Public disclosures should be made with sufficient clarity, timeliness, and inclusionary measures, to ensure that anyone can easily access information to make decisions and provide inputs.

Auditing: Governments and relevant regulatory bodies should conduct systematic and periodic audits and assessments of DPI systems to evaluate compliance with security standards, data protection regulations, and best practices. Proper audit logs should be maintained and made accessible to ensure appropriate oversight as a safeguard against unauthorized access by those without permission to operate DPI and manage data.

4. Strengthening Data Protection

DPI digitizes societal processes in a structured form and potentially makes data about such processes available to central authorities. This helps them obtain knowledge about the situation of a society or demographic in a particular societal area. Examples include research based on health records, assessing food stability or using public transport.

As a benefit, this enables a better understanding of the society and more focused government action to help certain demographics or to get a better understanding of public health. Complex phenomena become understandable when individual data sets cover a longer time frame, for example the impact of certain education initiatives on job opportunities or gender equality.

When such data is collected by DPI and processed for research (for example by third parties), privacy concerns arise. Governance should ensure that such secondary functions of DPI adhere to principles that respect human rights. The primary concern is that even pseudonymized data can be tied to a natural person whose records can be re-identified. Solely relying on pseudonymity would not be adequate protection. Relevant protections can be operationalized as:

Robust anonymization: Research about the collective situation of a demographic is not interested in individual data points about a natural person. Robust anonymization can achieve this by employing privacy-enhancing technologies such as synthetic data or differential privacy. Calculations can be done in protected environments separate from the third party, whereby the actual data is not transferred outside the DPI.

Agency: Consent about secondary usage of data – particularly if it includes transfers to third parties – is a vital pre-condition of trust. Without agency, individuals might choose to opt-out of using DPI. A system based on opting-in should employ fine-grain consent management and enable people to volunteer data for specific use cases.

Liability for misuse: Secondary uses of data obtained from DPI should fall under a liability regime to deter misuse, such as stalking, discrimination, or repurposing data for special interests outside of the public good. Technical protections that establish protocols for every interaction with the data sets should be established.

5. Effective Impact Assessment

Public sector impact assessment: Significant investment should be made in effectively implementing a legal framework to conduct timely system and subsystem assessments on issues such as data protection, algorithms and AI, interoperability, and human rights impact. Findings should be made public before systems or subsystems are put into effect, with only strictly limited exceptions to protect items such as: material prejudicial information tied to vital state interests, personally identifiable information, or critical cybersecurity concerns.

Industry impact assessment: Industry engaged in developing or implementing DPI should strictly adhere to prevailing guidelines and standards, comply with applicable laws, and conduct human rights due diligence and impact assessment. Human rights due diligence should cover adverse human rights impacts that the enterprise may cause or contribute to through its own activities or through those of its business relationships or supply chain.

6. Redress and Access to Justice

Effective redress is fundamental to the rule of law. Administrative procedures and recourse to judicial review should be made accessible for any decisions that implicate human rights, human development, and due process. All affected persons should have access to legal aid in adjudicating claims related to essential services, including, but not limited to, education, social protection, housing or financial services. Complaint and redress mechanisms should be accessible online and offline with transparent public reporting on outcomes. Judicial redress measures should allow for a pre-deprivation process for all essential services.

7. Monitoring and Evaluation

As DPI systems may entrust a significant amount of discretion over people's decisions and lives to technical implementers, transparent monitoring and evaluation mechanisms are vital. These mechanisms help identify patterns and practices that indicate a safeguard risk or failure. Regular public reporting on outcomes of monitoring and evaluation enables public auditing, builds trust, and guides the system towards continuous improvement.

8. Systems Approach to Maintenance

To realize the full potential of DPI and sustain its benefits, the implementing institutions should adopt a systems approach while tailoring the life cycle to context. Following initial investments, business models for DPI maintenance (including long-term costs for data-storage) should be developed. To achieve and sustain systemic change, local DPI providers, local digital ecosystems, including entrepreneurs, and researchers, should be trained and engaged through sustainable joint business models.

5.4 Sustained Governance

Every technological transformation brings opportunities and risks. Acceleration with DPI is uniquely challenging because it operates with a mandate from public authorities and is often implemented with a view to be scaled at population level. Unregulated operationalization of DPI, though systematic, would be dangerous in its impact on privacy, inclusion, equity, and the predictability of public institutions. Since DPI has the potential to significantly restructure our society, we should understand its implications and provide for the necessary governance frameworks to make it safe and inclusive. Sustained governance should ensure that laws and regulations are enforced and that the principles that underpin the mitigation and management of risks and which build safe and inclusive societies, are adhered to.

Sustained governance: Governance is the sum of mechanisms (institutional, formal, or otherwise) that serve the purpose of leveraging DPI that is trusted, inclusive, predictable, voluntary, and accessible. Governance is not only a pre-condition but should be sustained through the DPI life cycle. Sustained governance ensures that capacities and mitigations are in place and rules are upheld. Inclusion, safety, security and trustworthiness are not static concepts, but need to be adapted along the DPI life cycle. Changes in underlying technical realities and societal shifts have to be incorporated to sustain good governance.

As there is no one-size-fits-all DPI template for every country or region, subsidiarity – i.e., decision-making and governance at the appropriate decentralized level – becomes a priority for acceptance and trust. Governance can come from various levels (such as local self-governance, governmental, multi-stakeholder, and multilateral), which are differently suited to mitigate certain risks. Governance orients itself on assessment indicators that provide transparency about the system and guide the trajectory of its safe application and development. Therefore, the role of sustained governance is to adapt to the relevant risks and mitigation measures.

Governance Stakeholders

While governance processes are critical to success, identifying and proactively engaging with the key stakeholders of the DPI ecosystem, including capacity-

Types of Governance Stakeholders

- Governments
- Technology communities and companies
- Non-governmental organizations (NGOs)
- Businesses
- International development organizations
- Philanthropic foundations
- Think tanks and research institutions
- Researchers, academics, and domain experts
- Local ecosystems

building and resourcing, is essential to ensure that governance is comprehensive, balanced and sustainable throughout the DPI life cycle. DPI governance stakeholders include:

1. **Governments**, which are central to DPI governance. They establish policies, regulations, and frameworks that guide the development, deployment, and maintenance of DPI. Their role includes ensuring equitable access, safeguarding privacy, and promoting transparency.
2. **Technology communities and companies** actively participate in building, maintaining and evolving DPI and related physical-digital infrastructure. They also drive adoption due to their business interest in the new interactions, market expansion and access to open data.
3. **Non-governmental organizations (NGOs)** advocate for inclusive, privacy-respecting and rights-based DPI. They engage in proactive research, policy analysis, community outreach and on-the-ground monitoring to ensure that DPI serves the public interest.
4. **Businesses** invest in design, development, implementation and maintenance of DPI, and more importantly, develop and offer efficient existing or innovative new services to the public. Their expertise and operations influences DPI's effectiveness.
5. **International development organizations** like ITU, UNDP and World Bank actively support the adoption of DPI to enable growth and societal development, particularly in the Global South. They provide funding, technical assistance, and capacity-building programmes.
6. **Philanthropic foundations** contribute to DPI development by funding catalytic initiatives such as convenings, research, capacity-building,

technical assistance and assessments. Their efforts focus on bridging digital divides, ensuring safety, and fostering inclusivity.

7. **Think tanks and research institutions** engage in policy research and thought leadership. They analyse DPI's effectiveness and impact on the society, as well as assisting in shaping narratives, carrying out research, proposing best practices, and advocating for informed decision-making.
8. **Researchers, academics, and domain experts** provide valuable insights on risks and mitigation measures to build a safe and inclusive society. Their expertise informs DPI design, governance models, and strategies for addressing societal challenges.
9. **Local ecosystems** within countries—comprising start-ups, community organizations, and grassroots initiatives—contribute to DPI design and support adoption and sustenance of societal benefits. Their context-specific knowledge ensures relevance and responsiveness.

Governance Models of DPI Systems

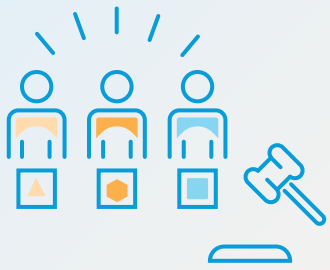
Governance models for DPI are pivotal in shaping how DPI systems operate, ensuring they are secure, accessible, and beneficial to all stakeholders. These models vary depending on the objectives, scale, and stakeholders of the DPI in question. Each model has relative strengths and weaknesses.

1. **Government-led**: Here state actors lead and regulate the various stages of the DPI life cycle with an emphasis on national security, economic interests and public welfare. Governments may work in partnership with private entities but retain significant control over policy and regulatory frameworks. This model is often seen in critical national infrastructures.
2. **Multi-stakeholder**: This brings together various groups, including government agencies, private sector participants, non-governmental organizations, and civil society, to collaborate in the governance process. It is based on the principle that the management of DPI benefits from the inclusion of diverse perspectives and insights of all stakeholders.
3. **Private sector-led**: This is when private companies develop and manage DPI systems with minimal government intervention – an example would be payment systems or cloud hosted services. While this can lead to rapid innovation and deployment of digital services, it raises concerns about market dominance, privacy, concentration risks, and equitable distribution of benefits.

4. **Public–private partnerships**: Involves collaboration between government and private sector to finance, develop, and manage DPI. Examples may be smart city infrastructures or open commerce projects. The aim here is to combine the efficiency and innovation of the private sector with the public accountability and oversight of the government.
5. **Community-based**: Emphasizes the role of local communities and user groups in the design, management and operation of DPI such as local digital ecosystems, digital commons initiatives or open-source communities. It is observed in open-source projects and community networks that often promote inclusivity, local engagement, and empowerment.
6. **Global governance bodies**: International organizations and consortia ensure global interoperability, standards, and security. Examples include the Internet Corporation for Assigned Names and Numbers (ICANN) for domain name management, or the International Telecommunication Union (ITU) for global telecom standards.

Each model presents advantages and challenges for safety and inclusion. Effective models strive to balance innovation and efficiency with accountability, equity, and protection of human rights. The choice of governance model or a combination thereof, can significantly impact the effectiveness of a DPI in serving the people in a safe and inclusive manner.

Types of Governance Models



- Government-led
- Multi-stakeholder
- Private sector-led
- Public–private partnerships
- Community-based
- Global governance bodies

Implementing Governance

1. **Rule of law and impartial and efficient enforcement**: Independent regulatory authorities should ensure that the ecosystem created with a DPI adheres to the laws and regulations that govern it. Both private and public (or hybrid) entities should be subject to a higher independent autonomous regulatory authority and advised by an independent multi-stakeholder committee of national and international members that includes experts and advocates.
2. **Subsidiarity principle and participation**: DPI governance should adhere to the subsidiarity principle, such that every decision should be made at the lowest level that involves all those affected. Local communities and underrepresented groups should be involved to ensure their voices are heard and accounted for. Their lived experiences need to be the starting point and include participatory decision-making throughout the life cycle of DPI.
3. **Transparency and capacity-building**: DPI systems come with their own risks, due to their unique characteristics and underlying technology. An early warning system should be developed; this can be achieved by reflecting upon past experiences through horizontal networking between public authorities, developing multi-stakeholder collaborative projects, ensuring open access to assessment indicators, promoting open standards, and funding research and civil society oversight.
4. **Failure resistance and human redress mechanisms**: Technology has inherent flaws and security is never a state, but a process. Effective means of redress and access to legal aid should be available to individuals in cases of fraud, identity theft, systemic mistakes or other harms. Governments should enable liability protections for individuals; multi-stakeholder participation should ensure independent oversight, testing and audits.
5. **Predictability and accountability for market actors**: It is critical to ensure that private sector use of DPI is predictable and regulated to protect privacy, especially when people are not in a position to refuse data-sharing. Government-led governance should guarantee that private and public sector interactions of DPI follow predictable rules that people trust. Public–private governance should verify that vendors regulate the functionalities they develop.
6. **Inclusivity in digital systems**: Embracing inclusivity in the design of DPI at a population level is a governance obligation. Government-led governance

should ensure rights to obtain DPI access, assure pricing, regulate personal information (including biometrics) and ensure independence from private interests. Stakeholders, including vulnerable groups, should be included in the design of the DPI to make sure the DPI adheres to their needs.

7. **Voluntary nature of DPI**: Upholding trust depends on systems where those who cannot access DPI are still given full access to the same services. Situations in which people are forced to use DPI-based services, especially when they lack access or digital literacy, causes exclusion and harms. Government or multilateral governance should ensure that public and private sector actors are obliged to offer alternative modes of using the services.
8. **Privacy-by-design guarantees**: DPI architecture should ensure that no unique persistent identifier for natural persons leaves the system. Vendors of DPI should provide for technical features that enable privacy-by-design guarantees to people. Government-led governance should provide a framework for safeguards as selection criteria for vendors. Multilaterals should require privacy-preserving guarantees for interoperability agreements.

Governance Implementations

- **Rule of law and impartial and efficient enforcement**
- **Subsidiarity principle and participation**
- **Transparency and capacity-building**
- **Failure resistance and human redress mechanisms**
- **Predictability and accountability for market actors**
- **Inclusivity in digital systems**
- **Voluntary nature of DPI**
- **Privacy-by-design guarantees**

Towards Evaluation and Assessment

Assessing successful implementation and effective governance of DPI relies on a set of agreed-upon principles and processes governed by measurable outcomes. During the inductive phase, the Working Groups identified an initial set of categories, groups and potential measures and indicators around which systematic evaluation and assessment mechanisms can be developed.

Three sample measures and indicators for each category / group are listed in the table on the next page. They would be refined, detailed and supported with evaluation and assessment frameworks during the deductive phase. The goal of this measurement framework is to inform the DPI design and implementation process, provide the opportunity to course-correct, and to propose options that can be used to develop country- and DPI-specific evaluation and assessment mechanisms.

Evaluation and Assessment for DPI Governance

Category	Group	Three Sample Measures and Indicators
Access and Redressal	Equitable and Voluntary Access	Percentage of population with DPI access limitations
		Percentage of services available in all official languages
		Number of services where use of DPI is mandatory
	Effective and Timely Redressal	Percentage of issues with high impact / high severity
		Average time to resolve complaints or requests
		Percentage of issues resolved to satisfaction / quality
Institutions and Processes	Institutional Robustness	Appropriate indicators of Rule of Law
		Appropriate indicators of regulatory controls
		Indicators of readiness across DPI life cycle
	Accountability and Transparency	Measures of accountability and transparency
		Readiness / capability to monitor and evaluate DPI
		Number of improvements based on participatory feedback
Law and Policies	Regulatory and Policy Effectiveness	Indicators of respect of the rule of law
		Implementation of privacy laws and regulations
		Number of policies / regulations embedded in DPI design
	Inclusiveness and Participation	Indicators of equality and non-discrimination
		Measures of inclusion at critical life cycle stages
		Measures of participation at critical life cycle stages
Technology Readiness	Responsibility and Trustworthiness	Indicators of responsible disclosure policies
		Degree of openness of DPI technology
		Technical measures of security, privacy, and ethics
	Data Handling Effectiveness	Regularity of audits / red-teaming exercises
		Indicators of regular and rigorous stress testing
		Degree of back up plans and data localization
	Resilience and Testing Effectiveness	Service blackouts / Down time of systems
		Degree and performance of redundancies
		Number and severity of security / other incidents
Market Dynamics	Innovation Ecosystem Diversity	Updated public registry of all with data access
		Number of new benefits from the innovation ecosystem
		Utilization of DPI in new product / service design
	Effectiveness of Capacity Building	Effective participation of all sectors in DPI life cycle
		Effective feedback loops to improve inclusion
		Effective feedback loops to improve safety

6.0 Next Steps

The next phase, the deductive phase, aims to create the DPI Safeguards framework with a solid foundation and enough flexibility to ensure DPI implementation in countries promotes sustainable growth and leads to safe and inclusive societies. With a bias for in-country implementation at the heart of this initiative, the next phase is organized around a nominal DPI life cycle, focused on fostering trust and effective multi-stakeholder participation throughout the journey of DPI adoption and maintenance.

Recognizing that the infrastructure approach to digitization affects diverse stakeholders, the next phase highlights how differences and gaps can be resolved, including strengthening mediation, redress, and iteration during the adoption journeys. During the deductive phase, the Working Groups will build on the foundations laid in this Interim Report, codifying participatory processes, effective practices (including capacity-building) and sustained governance (including robust assessments) across the entire DPI life cycle (including its potential interoperability with other systems and DPI).

Through the next phase, the Working Groups will be supported with in-country validations, global convenings, and insights from the International Organizations Consultative Group.

- **In-country validations**: Building on the inductive phase, the in-country engagements during the next phase will support the Working Groups to understand diverse country and stakeholder contexts during implementation. This includes surfacing instances of 'holding environments' where effective multi-stakeholder participation throughout the journey of DPI adoption can extend advice, validate, provide feedback and resolve differences.

- **Global convenings**: The Initiative will continue to invite governments, civil society organizations and private sector actors to help develop and refine the DPI Safeguards framework by including the voices of their respective communities. Please see the up-to-date global convenings calendar where connections have been initiated. Contact dpi-safeguards@un.org to request support with a convening in your community.
- **International Organization Consultative Group (IOCG)**: During the deductive phase, the IOCG's perspectives are indispensable in order to understand the practical implications and applicability of findings of the Interim Report. It ensures that the framework remains grounded and is informed by practical considerations and experiences from various international contexts.

As DPI operates in complex and dynamic societal ecosystems, feedback to the Interim Report from the wider group of stakeholders will be critical for the next phase. This will ensure that the development of the DPI Safeguards framework benefits from a wide range of perspectives, enriching the foundational principles with diverse viewpoints and experiences. We look forward to taking this journey together.

Annex 1

Resources for Further Reading

- Abbasi, S et al., (2023). *Framework for Digital Public Goods in Least Developed Countries.* vol., no., pp.1-15. IEEE. https://ieeexplore.ieee.org/document/10247189/authors
- Access Now (2024). *Digital Identity Toolkit.* https://www.accessnow.org/guide/digital-id-toolkit/
- Access Now (2023). *Past learnings must be 'at the heart of implementing' a digital identity system in Kenya.* https://www.accessnow.org/press-release/kenya-digital-identity-systems/
- Amnesty International (2020). *Amnesty International Calls for Ban on the Use of Facial Recognition Technology for Mass Surveillance.* https://www.amnesty.org/en/latest/research/2020/06/amnesty-international-calls-for-ban-on-the-use-of-facial-recognition-technology-for-mass-surveillance/
- Arraiza, MJ (2023). *Will Digital ID help Stateless People? The Threat of Digital Administrative Violence*. European Network on Statelessness. November. https://www.statelessness.eu/updates/blog/will-digital-id-help-stateless-people-threat-digital-administrative-violence
- Banco Central De Brasil (2024). Pix. https://www.bcb.gov.br/en/financialstability/pix_en
- Batra, A, Naik, AA and Thiagarajan K (2017). *E-Governance Maturity Framework*. eGov Foundation. https://egov.org.in/wp-content/uploads/2021/08/eGov-Maturity-Framework.pdf.
- Berkeley Law, International Human Rights Law Clinic (2023). *Digital Identity and the Legal Obligation to Conduct a Human Rights Impact Assessment in Kenya.* https://drive.google.com/file/d/1ozXd-H94x8p-zTKrtXAnpvEWlIzQtbmy/view
- Beckn Protocol. (N/d). Imagining energy with beckn. https://becknprotocol.io/imagining-energy-with-beckn-protocol/
- Beckn Protocol. (N/d). Reimagining e-commerce policies through open protocols. https://becknprotocol.io/reimagining-e-commerce-policies-through-open-protocols/
- Bill and Melinda Gates Foundation (2019). *Level One Project Guide*. https://www.leveloneproject.org/wp-content/uploads/2020/07/L1P_Guide_2019_Final.pdf
- Bingham, L (2023). *The Cart Before the Horse – A Kenyan Court Just Quashed a USD 95M Biometric Digital ID Project.* Voices at Temple Law, Temple University: Beasley School of Law. https://www2.law.temple.edu/voices/the-cart-before-the-horse-a-kenyan-court-just-quashed-a-usd-95m-biometric-digital-id-project/
- Bingham L, Cioffi K, Adamant V (2023). *Shaping Digital Identity Standards: Explainer and Recommendations.* Temple University Institute for Law, Innovation & Technology, NYU Digital Welfare State Project. https://www.digitalbenefitshub.org/resources/shaping-digital-identity-standards-explainer-and-recommendations
- Brinkerhoff, DW (2006). Accountability and good governance: Concepts and issues. *International Development Governance*. https://www.

researchgate.net/publication/329631689_Accountability_and_Good_Governance_Concepts_and_Issues
- British Post Office Scandal (https://en.wikipedia.org/wiki/British_Post_Office_scandal)
- Burt, C (2018). Vendor lock-in hindering African identity projects, Biometricupdate.com https://www.biometricupdate.com/201806/vendor-lock-in-hindering-african-identity-projects
- *BusinessLine* (2022). PCI calls for roll back of zero MDR in budget 2022-23. January 21. https://www.thehindubusinessline.com/money-and-banking/pci-calls-for-roll-back-of-zero-mdr-in-budget-2022-23/article64928074.ece
- Byers, S and Nurko, G (2021). *Cybersecurity Primer: How to Build Cybersecurity into USAID Programming.* USAID. https://www.usaid.gov/sites/default/files/2022-05/10-26-21_EXTERNAL_CyberPrimer-CLEARED-accessible.pdf.
- Cappa, C and Petrowski, N (2019). *Birth Registration for Every Child by 2030: Are We on Track?* UNICEF. https://www.unicef.org/rosa/media/5111/file
- Carse, A (N/d). Beyond the big ditch: Politics, ecology, and infrastructure at the Panama Canal. Cambridge, MA: MIT Press. https://mitpress.mit.edu/9780262537414/beyond-the-big-ditch/
- Cavoukian, A (2010). Privacy by design: The 7 foundational principles – implementation and mapping of fair information practices. Paper. https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf
- Cañares, M (2019). What do we mean by data empowerment? Medium. https://medium.com/data-empowerment/what-do-we-mean-by-data-empowerment-f842ef9880b
- CDPI (N/d). *DPI Tech Architecture Principles*. Centre for Digital Public Infrastructure. https://docs.cdpi.dev/the-dpi-wikipedia/dpi-tech-architecture-principles
- CDPI (N/d). *DPI and Private Competition*. Centre for Digital Public Infrastructure. https://docs.cdpi.dev/mythbusters-and-faqs/dpi-and-private-competition
- CDPI (N/d). *Diverse, Inclusive Innovation*. Centre for Digital Public Infrastructure. https://docs.cdpi.dev/the-dpi-wikipedia/dpi-tech-architecture-principles/diverse-inclusive-innovation
- CDPI (N/d). *DPI and Privacy / Security*. Centre for Digital Public Infrastructure. https://docs.cdpi.dev/mythbusters-and-faqs/dpi-and-privacy-security
- Chirchir, R and Barca, V (2019). *Building an Integrated and Digital Social Protection Information System.* Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH. https://www.giz.de/en/downloads/giz2019-en-integrated-digital-social-protection-information-system.pdf.
- Chowdhury, A (2023). Bangladesh's "phygital public infrastructure" bridges DPI theory and practice. a2i.
- https://a2i.gov.bd/bangladeshs-phygital-public-infrastructure-bridges-dpi-theory-and-practice/
- CIPESA (2023). Uganda's digital ID system hinders citizens' access to social services. https://cipesa.org/2023/10/ugandas-digital-id-system-hinders-citizens-access-to-social-services/.
- Clark, J (2019). *ID4D Practitioner's Guide Version 10.* World Bank. Washington, D.C. https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf.
- Data Prev. https://www.dataprev.gov.br
- Davis Center for Russian and Eurasian Studies. (2021). *Beyond the*

GovTech: The Pitfalls of Kazakhstan's Digitalization Agenda, in Digital Silk Road in Central Asia: Present and Future. Nargis Kassenova and Brendan Duprey (Eds.) https://daviscenter.fas.harvard.edu/sites/default/files/files/2021-10/Digital_Silk_Road_Report_2021.pdf#page=90

- Department of Homeland Security. *Privacy Impact Assessments*. https://www.dhs.gov/privacy-impact-assessments
- Dennis, JB (1975). "Modularity", in An Advanced Course in Software Engineering (Bauer, FL) (ed). Reprint of the First Edition. February 21 – March 3, 1972. Springer.
- Dencik, L and Sanchez-Monedero, J (2022). Data justice. *Internet Policy Review.* https://policyreview.info/articles/analysis/data-justice
- Defindia.org: https://www.defindia.org/wp-content/uploads/2023/07/T20_PB_TF2_205_DPI-Indian-Experience.pdf.
- Differential Privacy: https://en.wikipedia.org/wiki/Differential_privacy
- DPGA (2022). GovStack Definitions: Understanding the relationship between Digital Public Infrastructure, building blocks & Digital Public Goods. Paper. Digital Public Godds Alliance. https://digitalpublicgoods.net/DPI-DPG-BB-Definitions.pdf
- Eaves D, Sandman, J (N/d). What is Digital Public Infrastructure?. Co-develop. https://www.codevelop.fund/insights-1/what-is-digital-public-infrastructure
- Eaves D, Mazzucato M and Vasconcellos B (2024). *Digital Public Infrastructure and Public Value: What is 'Public' About DPI?* UCL Institute for Innovation and Public Purpose. https://www.ucl.ac.uk/bartlett/public-purpose/publications/2024/mar/digital-public-infrastructure-and-public-value-what-public-about-dpi
- Eke D, et al., (2022). Nigeria's Digital Identification (ID) management rogram: Ethical, legal and socio-cultural concerns. *Journal of Responsible Technology*. Vol 11. October 2022. 100039. https://www.sciencedirect.com/science/article/pii/S2666659622000166
- Epicenter.Works (2024). *Analysis of Privacy-by-Design EU Legislation on Digital Public Infrastructures*. https://epicenter.works/content/analysis-of-privacy-by-design-eu-legislation-on-digital-public-infrastructures
- European Commission, National Institute of Standards and Technology (2023). *Digital Identity Mapping Exercise Report.* https://futurium.ec.europa.eu/system/files/2023-12/EU-US%20TTC%20WG1_Digital_Identity_Mapping_Report_Final%20Draft%20for%20Comment_22122023.pdf
- EUR-Lex (2022). Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.265.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A265%3ATOC
- EUR-Lex (2023). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001
- Financial Action Task Force (2020). *Digital Identity.*
- Folz, J (2022). *FOSS is Necessary But Not Sufficient: Lessons from the History and Politics of the Free and Open-Source Software Movement in India*. Digital Futures Lab. https://digitalfutureslab.notion.site/FOSS-is-Necessary-but-Not-Sufficient-Lessons-from-the-History-and-Politics-of-the-Free-and-Open-Sou-94dd0df0320b480ab9b5d7b6da6defc4
- Foster, C (2022). Intellectual property rights and control in the digital economy: Examining the expansion of M-Pesa. *The Information Society*. 40(1). https://www.tandfonline.com/doi/full/10.1080/01972243.2023.225

9895
- Ganapathy, A and Mahindru, T (2023). *Gender by design: Principles of gender-responsive Public Digital Infrastructure.* IT for Change. Paper. https://itforchange.net/index.php/gender-by-design-principles-for-gender-responsive-public-digital-infrastructure
- Geiger, G (2023). How we did it: Unlocking Europe's welfare fraud algorithms. Journalist Resource. Pulitzer Center. https://pulitzercenter.org/how-we-did-it-unlocking-europes-welfare-fraud-algorithms
- Group of 20 Indonesia Infrastructure Working Group (2022). *Digital Infrastructure Finance: Issues, Practices and Innovations.* G20 and Asian Infrastructure Investment Bank.
- Gupta, A and Narayan, A (2021). *Moving to Offline And On-Spot CoWIN Registration: Away From the Not-So-Common Service Centers*. Dvara Research. https://dvararesearch.com/moving-to-offline-and-on-spot-cowin-registration-away-from-the-not-so-common-service-centres/
- Global Partnership for Financial Inclusion (2023). *G20 Policy Recommendations for Advancing Financial Inclusion and Productivity Gains through Digital Public Infrastructure.* https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099092023121016458/p178703046f82d07c0bbc60b5e474ea7841
- Goodman, N and Morris, M (2017). Banking status and financial behaviors of adults with disabilities. Findings from the 2017 FDIC National Survey of Unbanked and Underbanked households and Focus Group Research. National Disability Institute. https://www.nationaldisabilityinstitute.org/wp-content/uploads/2019/11/ndi-banking-report-2019.pdf
- Goodwin-Groen, R and Klapper, L (2023). *Reaching Financial Equality for Women.* Better than Cash Alliance. https://www.betterthancash.org/news/digital-financial-services-can-help-bring-millions-of-women-into-the-workforce
- Govstack (2022). Digital public infrastructure, building blocks, and their relation to digital public goods. https://www.govstack.global/news/digital-public-infrastructure-building-blocks-and-their-relation-to-digital-public-goods/
- Govtech Singapore (2024). Singapore Government Tech Stack (SGTS). https://www.tech.gov.sg/products-and-services/singapore-government-tech-stack/
- GOV.UK (2023). UK digital identity and attributes trust framework beta version *(0.3)*. https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-beta-version/uk-digital-identity-and-attributes-trust-framework-beta-version#introduction.
- GSMA (2019). *The Digital Lives of Refugees: How Displaced Populations Use Mobile Phones and What Gets in the Way.*
- Islamic Development Bank. *Digital Bangladesh: High Speed Connectivity via Mobile Phones and the Internet.* https://www.isdb.org/case-studies/digital-bangladesh-high-speed-connectivity-via-mobile-phones-and-the-internet.
- Islamic Development Bank (2023). *Bridging the Digital Divide to Accelerate Development.* https://www.isdb.org/news/bridging-the-digital-divide-to-accelerate-development.
- Hersey, F (2021). Urgent call to erase biometric, digital ID databases in Afghanistan. Biometricupdate.com. Biometric Update. 27 August. https://www.biometricupdate.com/202108/urgent-call-to-erase-biometric-digital-id-databases-in-afghanistan
- Hsiao, DK (1992). Federated databases and systems: Part I—A tutorial on their data sharing. *The VLDB Journal*. 1.

- Hossain, N et al., (2024). The politics of complaint: A review of the literature on grievance redress mechanisms in the global South. *Policy Studies*. https://accountabilityresearch.org/wp-content/uploads/2023/06/The-politics-of-complaint-a-review-of-the-literature-on-grievance-redress-mechanisms-in-the-global-South.pdf
- IFRC (2020). Growing up 2030 in a digital world. *Enabling Digital Health Futures in Humanitarian Settings.*
- iSPIRT Foundation (N/d). *Data Empowerment - a Techno Legal Approach*. https://drive.google.com/file/d/1xVKRtxeOIEzBUOLJUeCh0RVxX5vaZIz8/view
- IT for Change (2023). Gender by Design: Principles of gender-responsive Public Digital Infrastructure. Research Paper. https://itforchange.net/index.php/gender-by-design-principles-for-gender-responsive-public-digital-infrastructure
- India Stack: https://indiastack.org
- Institut Statelessness and Inclusion (N/d). South Africa high court declares ID blocking unjust and unconstitutional. https://www.institutesi.org/news/south-africas-high-court-declares-id-blocking-unjust-and-unconstitutional
- Jamaicans for Justice (2024). Robinson, Julian v. Attorney General of Jamaica. https://jamaicansforjustice.org/download/julian-robinson-v-ag/.
- Justice K.S. Puttaswamy and Anr. vs. Union of India (UOI) and Ors (2018). https://privacylibrary.ccgnlud.org/case/justice-ks-puttaswamy-and-ors-vs-union-of-india-uoi-and-ors?searchuniqueid=111790
- Chaos Computer Club (N/d). Hacker Ethics. (https://www.ccc.de/en/hackerethik)
- Kalaf, E (2021). Legal identity, race and belonging in the Dominican Republic. Anthem Press. https://anthempress.com/anthem-series-in-citizenship-and-national-identities/legal-identity-race-and-belonging-in-the-dominican-republic-hb
- Kashem, A (2023). Govt to create Tk100cr fund for Smart Bangladesh vision. The Business Standard. 30 May. : https://www.tbsnews.net/economy/budget/govt-create-tk100cr-fund-smart-bangladesh-vision-640462
- Kjørven, ME (2020). Who pays when things go wrong? Online financial fraud in Scandinavia and Europe. *European Business Law Review.* 31(1).
- Koo Wilkens, P and Shreeti V (2024). Fast payments: Design and adoption. *BIS Quarterly Review*. https://www.bis.org/publ/qtrpdf/r_qt2403c.htm
- LINDDUN (N/d). *A Framework for Privacy Threat Modelling.* https://linddun.org/
- Manby, B (2021). The Sustainable Development Goals and 'legal identity for all': 'First, do no harm'. *World Development.* Vol 139. March 2021.105343. https://www.sciencedirect.com/science/article/abs/pii/S0305750X20304708
- UNHCR (N/d). *Connecting with Confidence: Managing Digital Risks to Refugee Connectivity.* UNHCR Innovation Service.
- Ministry of Economic Affairs and Communication, Republic of Estonia (2011). *Interoperability of the State Information System.* www.stat.ee/sites/default/files/2022-11/Estonian%20IT%20Interoperability%20Framework%20-%20Abridgement%20of%20Version%203.0.pdf
- Ministry of Electronics and Information Technology (2023). Cabinet approves the incentive scheme for promotion of RuPay debit cards and low-value BHIM-UPI transactions (P2M). https://pib.gov.in/PressReleasePage.aspx?PRID=1890314.
- Ministry of Finance (2023). Paradigm shift in digital transactions in

India with growth of more than 200% in digital payment volume during the last four years since 2018–19. Press Release. Press Information Bureau. Government of India. https://pib.gov.in/PressReleseDetailm.aspx?PRID=1906541
- Mojaloop: mojaloop.io
- MOSIP: mosip.io
- Nash, J (2021). Potentially devastating digital ID hack in Argentina could have many ripples. Biometricupdate.com. https://www.biometricupdate.com/202110/potentially-devastating-digital-id-hack-in-argentina-could-have-many-ripples
- National Institute of Standards and Technology (N/d). NIST Cybersecurity Framework. https://www.nist.gov/itl/smallbusinesscyber/nist-cybersecurity-framework-0
- National Payments Corporation of India (2024). Unified payments interface. https://www.npci.org.in/what-we-do/upi/product-overview
- National Payments Corporation of India (2024). UPI ecosystem statistics. https://www.npci.org.in/what-we-do/upi/upi-ecosystem-statistics
- Next Generation Internet: https://www.ngi.eu/
- NHS England (2023). *Inclusive Digital Healthcare: A Framework for NHS Action on Digital Inclusion.* https://www.england.nhs.uk/long-read/inclusive-digital-healthcare-a-framework-for-nhs-action-on-digital-inclusion/.
- Nordhaug, ML and Harris, L (N/d). Digital public goods: Enablers of digital sovereignty. OECDiLibrary. : https://www.oecd-ilibrary.org/sites/c023cb2e-en/index.html?itemId=/content/component/c023cb2e-en#:~:text=linklink%20copied!-,Digital%20public%20goods%20save%20resources%2C%20build%20trust%20and%20enable%20scaling,Opensource%2C%20n.d.%5B10%5D
- OECD (2020). The OECD digital government policy framework: Six dimensions of a digital government. OECD Public Governance. Policy Paper No. 02. OECD Publishing. Paris. https://www.oecd-ilibrary.org/governance/the-oecd-digital-government-policy-framework_f64fed2a-en.
- OECD (2021). *Smart Policies for Smart Products: A Policymaker's Guide to Enhancing the Digital Security of Products.* https://web-archive.oecd.org/2021-02-08/579066-smart-policies-for-smart-products.pdf.
- OECD (2021). Understanding the digital security of products: An in-depth analysis. OECD Digital Economy Papers. No. 305. OECD Publishing. Paris. https://www.oecd-ilibrary.org/science-and-technology/understanding-the-digital-security-of-products_abea0b69-en.
- OECD (2021). Enhancing the digital security of products: A policy discussion. OECD Digital Economy Papers. No. 306. OECD Publishing. Paris. https://www.oecd-ilibrary.org/science-and-technology/enhancing-the-digital-security-of-products_cd9f9ebc-en. OECD (2023). Recommendation of the Council on OECD legal instruments the governance of digital identity. OECD/LEGAL/0491. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0491.
- OECD (2022). Recommendation of the Council on Digital Security Risk Management, OECD/LEGAL/0479. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0479.
- OECD (2022). Recommendation of the Council on the Digital Security of Products and Services. OECD/LEGAL/0481. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0481.
- OECD (2024). 2023 OECD Digital Government Index: Results and key findings. OECD Public Governance Policy Papers. No. 44. OECD Publishing.

Paris. https://www.oecd.org/publications/2023-oecd-digital-government-index-1a89ed5e-en.htm.
- Open Future EU (2022). *Towards Public Digital Infrastructure: A Proposed Governance Model.* Bego, K (2022). NGI Forward. https://openfuture.eu/wp-content/uploads/2022/12/TowardsPublicDigitalInfrastructure_v0.2.pdf
- Open Future EU (2022). *Towards A Sovereign Digital Infrastructure of Commons.* https://openfuture.eu/wp-content/uploads/2022/12/report_of_the_european_working_team_on_digital_commons_digital_assembly_june_2022_wnetherlands_cle843dbf.pdf
- Open Gambia Network (2023). Introducing an Open Network in the Gambia to accelerate innovation and foster equitable, inclusive, and open access to digital services across sectors. Concept Note. https://oga.gm/oga/ogaconceptNote.pdf
- Oxfam, The Engine Room (2019). *Biometrics in the Humanitarian Sector*. https://oxfamilibrary.openrepository.com/bitstream/handle/10546/620454/rr-biometrics-humanitarian-sector-050418-en.pdf;jsessionid=4C8BFD2CEB040901883571B04902DABD?sequence=1
- Panday, J (2023). *India Stack: Public-Private Roads to Data Sovereignty*. Georgia Institute of Technology. School of Public Policy.
- Panijar, T and Waghre, P (2023). *Open Network for Digital Commerce (ONDC): An Explainer.* Internet Freedom Foundation. https://internetfreedom.in/ondc-an-explainer/
- Paul, Yesha T (2019). Centre for Internet and Society. *Digital Identities: Design and Uses.* https://digitalid.design/decisions-guide/governance-framework.html.
- Prime Minister's Office, Singapore (2023). PM Lee Hsien Loong at the launch of the PayNow-UPI linkage. Press Release. https://www.pmo.gov.sg/Newsroom/PM-Lee-Hsien-Loong-at-the-Launch-of-PayNow-UPI-Linkage-Feb-2023
- Principles for Digital Development (2024). https://digitalprincip.wpengine.com/home.
- Privacyinternational.org. (2022). Data protection impact assessments and ID systems: The 2021 Kenyan ruling on Huduma Namba. https://privacyinternational.org/news-analysis/4778/data-protection-impact-assessments-and-id-systems-2021-kenyan-ruling-huduma
- Prompt Pay: https://www.bot.or.th/en/financial-innovation/digital-finance/digital-payment/promptpay.html#accordion-15b3f8d52f-item-cb3c3ef862
- R3D et al., (2021). *Acción de inconsittucionalidad 82/2021 y Su acumulada 86/2021, Asunto: Se Presenta Escrito en Calidad de Amicus Curaiae.* https://r3d.mx/wp-content/uploads/Amicus-PANAUT-08022022.pdf.
- Rathi, A (2019). Is India's digital health system foolproof? *Economic and Political Weekly.* 54, no. 47. : https://www.epw.in/engage/article/indias-digital-health-paradigm-foolproof
- Raja Samant Deepti (2016). *Bridging the Disability Divide through Digital Technologies*. World Bank Group. https://thedocs.worldbank.org/en/doc/123481461249337484-0050022016/original/WDR16BPBridgingtheDisabilityDividethroughDigitalTechnologyRAJA.pdf
- Red Team: https://en.wikipedia.org/wiki/Red_team
- Reserve Bank of India (2016). *Annual Report 2015-2016*. https://rbidocs.rbi.org.in/rdocs/AnnualReport/PDFs/0RBIAR2016CD93589EC2C4467793892C79FD05555D.PDF.
- Reserve Bank of India (N/d). *Payment System Indicators.* https://www.rbi.org.in/Scripts/PSIUserView.aspx?Id=32
- *Reuters* (2022). India extends deadline to levy cap on digital payment

transactions. 2 December. https://www.reuters.com/technology/india-extends-deadline-levy-cap-digital-payment-transactions-2022-12-02/
- Ribes, D and Finholt, TA (2009). The long now of technology infrastructure: Articulating tensions in development. *Journal of the Association for Information Systems*. *https://aisel.aisnet.org/jais/vol10/iss5/5/*
- Sahamati: https://sahamati.org.in/governance/
- Singh, M (2022). India won't enforce payments market share cap until 2025 in win for Google and Walmart. *Tech Crunch*. December 2022. https://techcrunch.com/2022/12/02/india-wont-enforce-market-share-cap-on-upi-until-2025-in-a-win-for-google-and-walmart/
- Sharma, Shruti, and Camilo Tellez-Merchan (2024). *UN Principles for Responsible Digital Payment: Technical Note - Make recourse clear, quick and responsive.* Better Than Cash Alliance.
- Seth, A et al., (2023). A governance framework for Digital Public Infrastructure: Learning from the Indian Experience. T20. Policy Brief.
- Synthetic Data: https://en.wikipedia.org/wiki/Synthetic_data
- Tazama: tazama.org
- *Indian Express* (2017). Union Budget 2017: Govt announces two new incentives to promote BHIM app. 1 February. https://indianexpress.com/article/technology/tech-news-technology/union-budget-2017-bhim-app-being-used-by-125-lakh-people/
- The Alan Turing Institute (2021). *Facets of Trustworthiness in Digital Identity Systems*. https://www.turing.ac.uk/sites/default/files/2021-05/technical_briefing-facets_of_trustworthiness_in_digital_identity_systems.pdf
- The Engine Room (2020). *Understanding the Lived Effects of Digital ID: A Multi-Country Study*. https://digitalid.theengineroom.org/assets/pdfs/200123_FINAL_TER_Digital_ID_Report+Annexes_English_Interactive.pdf
- The European High Performance Computing Joint Undertaking: https://eurohpc-ju.europa.eu/index_en
- The European Quantum Communication Infrastructure (EuroQCI) Initiative: https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci)
- The Commonwealth: https://thecommonwealth.org/news/commonwealth-joins-forces-global-tech-organisations-empower-commonwealth-citizens-ai
- TaxGuru (2019). President assents finance (No 2) Act 2019. India. https://taxguru.in/income-tax/president-assents-finance-no-2-act-2019.html.
- The Open Quantum Institute: https://oqi.gesda.global/
- The Skill Hub: https://sipshalainstitute.com/
- *The Wire* (2017). Activists slam mandatory linking of Aadhaar to health services after woman denied abortion. 1 November. https://thewire.in/government/activists-slam-mandatory-linking-aadhaar-health-services-woman-denied-abortion
- United Kingdom - National Data Guardian for Health and Social Care (2022). *What Do We Mean by Public Benefit? Evaluating Public Benefit When Health and Adult Social Care Data Is Used for Purposes beyond Individual Care*. Guidance document. https://www.gov.uk/government/publications/what-do-we-mean-by-public-benefit-evaluating-public-benefit-when-health-and-adult-social-care-data-is-used-for-purposes-beyond-individual-care
- United Nations: *The Three Pillars*. https://www.un.org/ruleoflaw/the-three-pillars/
- United Nations Office of the Secretary-General's Envoy on Technology

(OSET) and the United Nations Development Programme (2024). *Digital Public Infrastructure: Universal Safeguards.* https://www.dpi-safeguards.org/
- UNDP (2021). *Human Rights Due Diligence: An Interpretive Guide*. https://www.undp.org/sites/g/files/zskgke326/files/2022-10/HRDD%20Interpretive%20Guide_ENG_Sep%202021.pdf
- UNDP (2023). *The DPI Approach: A Playbook*. https://www.undp.org/publications/dpi-approach-playbook
- UNDP (2024). Digital Public Infrastructure. https://www.undp.org/digital/digital-public-infrastructure
- UNDP (2024).*"5-Do No Harm"*. https://www.undp.org/digital/standards/5-do-no-harm
- UNDP (2023). *The Human and Economic Impact of Digital Public Infrastructure*. https://www.undp.org/publications/human-and-economic-impact-digital-public-infrastructure
- UNDP: Digital X. (N/d). Mizan 2: Facilitating access to justice, transparent judicial process, and comprehensive data to policy makers. https://digitalx.undp.org/mizan-2_1.html
- UNDP (2022). *UNDP Model Governance Framework for Digital Legal Identity.* https://www.governance4id.org/.
- UNDP (2023). Digital Transformation Framework. https://www.undp.org/digital/transformations.
- UNDP (2024). *A Shared Vision for Digital Technology and Governance: The role of governance in ensuring digital technologies contribute to development and mitigate risk*. https://www.undp.org/publications/dfs-shared-vision-digital-technology-and-governance-role-governance-ensuring-digital-technologies-contribute-development-and-mitigate-risk
- UNHCR Innovation Service – Digital Innovation Program (2020). *Displaced and Disconnected- Americas – Part 1 (Brazil, Chile, Colombia, Ecuador, and Peru).*
- UNHCR Innovation Service – Digital Innovation Program. *(2020). Displaced and Disconnected - Global (20 countries).*
- UNHCR Innovation Service –Digital Innovation Program (2022). *Displaced and Disconnected- Indonesia.*
- UNHCR Innovation Service – Digital Innovation Program. *(2022). Displaced and Disconnected- Americas – Part 2. (Argentina, Costa Rica, Dominican Republic, Guatemala, Mexico, Trinidad and Tobago).*
- UNHCR Innovation Service – Digital Innovation Program (2023). *Displaced and Disconnected- Malaysia.*
- UNHCR Innovation Service – Digital Innovation Program. *(2023). Displaced and Disconnected - Middle East and North Africa*
- UNHCR Innovation Service – Digital Innovation Program. (2023). *Displaced and Disconnected - Philippines.*
- UNICEF (2022). *Summative Evaluation of Digital Birth Registration Programme (2017–2021).*
- Unwanted Witness (2022) HEAPI and Initiative for Social and Economic Rights. Press Statement: Civil society sues government over Ndaga Muntu national ID: Mandatory digital ID threatens lives! https://www.unwantedwitness.org/download/Digital-ID-Litigation-_-PRESS-STATEMENT-FINAL.pdf
- Van Teeffelen, J and Baud, I (2011). Exercising citizenship: Invited and negotiated spaces in grievance redressal systems in Hubli-Dharwad. *Environment and Urbanisation Asia.* 2(2).
- Vally, N (2016). Insecurity in South African social security: An examination

of social grant deductions, cancellations, and waiting. *Journal of Southern African Studies* 42.

- Varma, P (N/d). *Driving Inclusion & Innovation at Scale: Digital ID as a Core DPI Building Block*. Indiastack. https://www.indiastack.global/wp-content/uploads/2023/02/Dr-Pramod-Verma-ID-Session.pdf
- Vishwakarma S et al., (2022). E-waste in Information and Communication Technology Sector: Existing scenario, management schemes and initiatives. *Environmental Technology and Innovation.* Vol 27.
- Wegner, P (1996). *Interoperability*. ACM Computing Surveys 28.
- World Bank (2022). A digital stack for transforming Service Delivery: ID, payments, and data sharing. Practitioner's Note. Washington, D.C. https://documents1.worldbank.org/curated/en/099755004072288910/pdf/P1715920edb5990d60b83e037f756213782.pdf
- World Bank (2022). *Next Generation G2P Payments: Building Blocks of a Modern G2P Architecture*. Washington, D.C. https://documents1.worldbank.org/curated/en/099600110202238143/pdf/P173166068e4220430a0ff03279b01c83db.pdf.
- World Bank (2017). Social registries for social assistance and beyond: A guidance note & assessment tool. Washington, D.C. https://documents1.worldbank.org/curated/ar/698441502095248081/pdf/117971-REVISED-PUBLIC-Discussion-paper-1704.pdf.
- World Bank Group and ID4D Initiative (N/d). Understanding people's experiences with identification: A guide for qualitative end-user research on ID. *https://documents1.worldbank.org/curated/pt/795541561701481546/pdf/Understanding-People-s-Experiences-with-Identification-A-Guide-for-Qualitative-End-User-Research-on-ID.pdf*
- World Bank (2019). *Global ID Coverage, Barriers, and Use by the Numbers: An In-Depth Look at the 2017 ID4D-Findex Survey.* Washington, D.C. https://openknowledge.worldbank.org/server/api/core/bitstreams/877144e7-84ba-5850-b4bd-6f5a04219e53/content
- World Bank (2021). *Principles on Identification for Sustainable Development: Toward the Digital Age.* Washington, D.C. https://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf
- World Economic Forum (2024). Digital public infrastructure – blessing or curse for women and girls? 5 March. WEF: Digital public infrastructure – blessing or curse for women and girls?
- World Economic Forum (2023). *Digital Transition Framework: An Action Plan for Public–Private Collaboration.* Cologny, Geneva. https://www3.weforum.org/docs/WEF_Digital_Transition_Framework_2023.pdf
- X-Road: https://x-road.global/
- Zannata F et al., (2024). *Emerging Trends in the Regulation of Platform Work in Brazil: A Preliminary Report*. https://www.dataprivacybr.org/wp-content/uploads/2024/03/regulation-of-platform-work_bydataprivacybrasil.pdf

Annex 2

DPI Safeguards Working Group Members

The experience and expertise of the DPI Safeguards' Working Group members range from, but is not limited to, multiple stages of the DPI life cycle to cybersecurity to open-source technologies and Artificial Intelligence (AI). They have come together as volunteers, focused on developing an implementable framework for leveraging DPI to build a safe and inclusive society and accelerate the achievement of the Sustainable Development Goals (SDGs).

- André Xuereb
- Angelina Fisher
- Anir Chowdhury
- Anit Mukherjee
- Armando Manzueta
- Assane Gueye
- Ben Le Roy
- Bilal Mateen
- Björn Richter
- CK Cheruvettolil
- Catherine Highet
- Cesar Perez
- Chris Mahony
- Clélia Cothier
- Fabro Steibel
- Giulia Fanti
- Hilda Mwakatumbula
- Janaina Costa
- José Arraiza
- Kasim Sodangi
- Kim Mallalieu
- Konstantin Peric
- Laura Bingham
- Laura O'Brien
- Lea Gimpel
- Liam Maxwell
- Linda Bonyo
- Maria Luciano
- Marte Eidsand Kjørven
- Matthew McNaughton
- Moctar Yedaly
- Monica Greco
- Mouloud Khelif
- Mphatso Augustine Sambo
- Priya Jaisinghani Vora
- Rahul Matthan
- Robert Ochola
- Sanjay Purohit
- Sheryl Gutierrez
- Siim Sikkut
- Thomas Lohninger
- Urvashi Aneja
- Ville Sirviö
- Yuliya Shlychkova

Annex 3

International Consultative Working Group

The International Organizations Consultative Group will comprise entities that are involved in implementing and shaping development agendas globally, regionally and locally, at a country or a state level. This Group plays a pivotal co-creation role in developing, validating, and implementing the framework.

- Asian Development Bank (ADB)
- African Development Bank (AFDB)
- European Bank for Reconstruction and Development (EBRD)
- Islamic Development Bank (IsDB)
- International Telecommunication Union (ITU)
- Organisation for Economic Co-operation and Development (OECD)
- Office of the United Nations High Commissioner for Human Rights (OHCHR)
- United Nations High Commissioner for Refugees (UNHCR)
- United Nations Children's Fund (UNICEF
- United Nations University (UNU)
- Better Than Cash Alliance (UN)
- World Bank

Annex 4

Working Group Organization and Key Themes

Through the inductive phase, the DPI Safeguards initiative engaged with six Working Groups. Each Working Group was dedicated to one of the six key focus areas: principles, operationalization, governance, technical aspects, normative frameworks, and organizational structures, with continuous cross-validation of findings between them.

Each Working Group engaged with appropriate stakeholders for in-depth analysis of their needs, experiences and perspectives. Intentionally, this approach encouraged overlapping areas of research that fostered cross-validation and promoted the sharing of knowledge and insights. This was very important for achieving comprehensive coverage and accuracy in the investigation of the designated areas during the inductive phase.

Risk dimensions: Three categories of risk were identified as being critical and warranting close examination. These included technical, normative, and organizational risks. The dimensions of risk are listed on the next page.

Mitigation dimensions: Besides identifying and categorizing risks within the methodology, a key focus was placed on controlling these risks across various dimensions of mitigation during the DPI implementation life cycle. These mitigation levels represent critical junctures where targeted measures and actions can significantly reduce the likelihood and impact of risk occurring.

TECHNICAL

Strategy and Design: The initial planning and design of Digital Public Infrastructure. It includes setting objectives, identifying stakeholders, and deciding on technologies and project structure.

Implementation: The technological components of DPI, including hardware, software, and networking.

Operational: Day-to-day functioning, management, and maintenance of DPI, ensuring that the infrastructure runs smoothly and effectively on a regular basis.

Structural: The organizational and architectural setup of DPI – the physical and logical layout of the infrastructure, including its scalability, security, and accessibility.

Systemic: How different components of DPI integrate and interact within a larger system. This considers the overall architecture and interoperability of various digital systems and services.

NORMATIVE

Legal: The legal framework, regulations, and compliance standards that govern DPI. This includes considerations of law that impact how digital infrastructures are developed, used, and managed

Ethical: Moral implications and responsibilities associated with DPI. This involves considering the impact of digital infrastructure on society and individuals, focusing on issues like privacy, equity, and access.

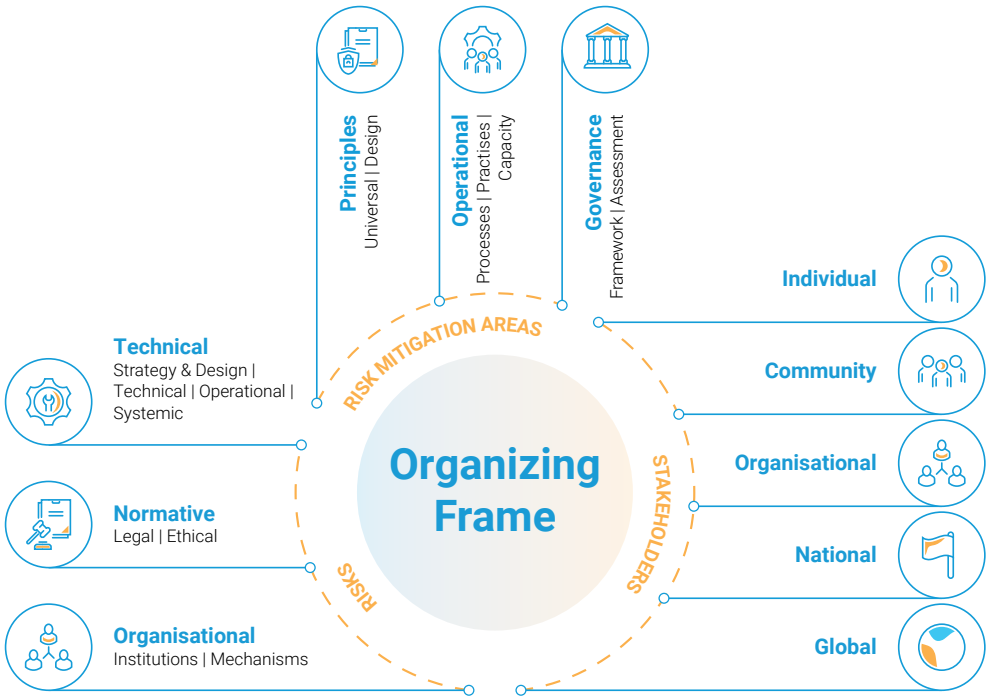
ORGANIZATIONAL

Institutional: Policies, governance, and the roles of various entities (such as government bodies, private organizations, and NGOs) in managing and regulating DPI. This includes how the infrastructure is overseen and the frameworks that guide evolution and usage.

Impact spectrum: From individual to global: It is important to acknowledge that risks can impact different groups/levels. These may be categorized as:

1. Individual: Risks that directly affect individuals or stakeholders.
2. Community: Risks that have implications for specific communities or social groups.
3. Institutional: Risks that impact organizations or institutions, internally or externally.
4. National: Risks with broader consequences on policies, economies, national security.
5. Global: Risks that impact international relations, global markets, or the environment.

This layered approach to classifying risk groups / levels adds another dimension to the comprehensive risk mitigation strategy, ensuring a nuanced and thorough consideration of potential impacts across various spheres of influence.



Annex 5

Terms of Reference for the Working Groups

Background: Through multi-stakeholder cooperation, the Digital Public Infrastructure Safeguards Initiative aims to promote safe and inclusive adoption of DPI to accelerate progress on the SDGs. Stewarded by the United Nations Secretary-General's Envoy on Technology (OSET) and the United Nations Development Programme (UNDP) as a public good, this initiative will develop the first global DPI Safeguards Framework and catalyze its implementation across countries by stakeholders to accelerate the SDGs. This is aligned with the United Nations Secretary General's (UNSG) Policy Brief on the Global Digital Compact (GDC), which emphasizes the need for common DPI frameworks to accelerate progress on the SDGs while mitigating the risks.

Objective: The DPI Safeguards Initiative Working Groups (WGs) will provide diverse interdisciplinary perspectives, undertake analysis of existing and emerging DPI systems, and advance recommendations to develop a global framework for safe, secure, and sustainable DPI adoption and implementation in countries.

Membership: Selected by OSET and UNDP from the wide range of open nominations received from the general public, WG members include diverse individuals from governments, private sector, civil society, and academia. The composition will be balanced by gender, age, geography, and expertise related to DPI. The WG members will serve in their personal capacity, dedicating approximately 8 to 12 hours monthly.

Structure: The WGs will be supported by the staff of OSET, UNDP and volunteer knowledge partners. Two rapporteurs chosen from the WG members will help finalize the recommendations. A group of experts from international organizations active in DPI will separately provide inputs from their perspective. Inputs from in-country implementers and regional convenings will be made available to WG as feedback to improve the draft framework.

Deliverables and process: Each WG will produce documents with detailed analysis and recommendations based on the specific WG scope of work. The process will include cross-validation of findings between WGs. The support team will synthesize and compile all documents, feedback, and input into an evolving framework that shall be shared publicly. The framework's public launch is expected at the Summit of the Future in September 2024. The WGs shall be convened until 31 December 2024 and will comprise both in-person and online meetings.

Framework purpose: This framework is intended to be used by countries, the United Nations and its partners in supporting countries on their DPI journeys. The final framework is designed equally for use by government actors, civil society organizations, the private sector and other DPI ecosystem participants to design, implement and scale safe and inclusive DPI in their respective countries. The framework will serve as a practical guide to assess, design, and course-correct during the various stages of a country's DPI journey.

.

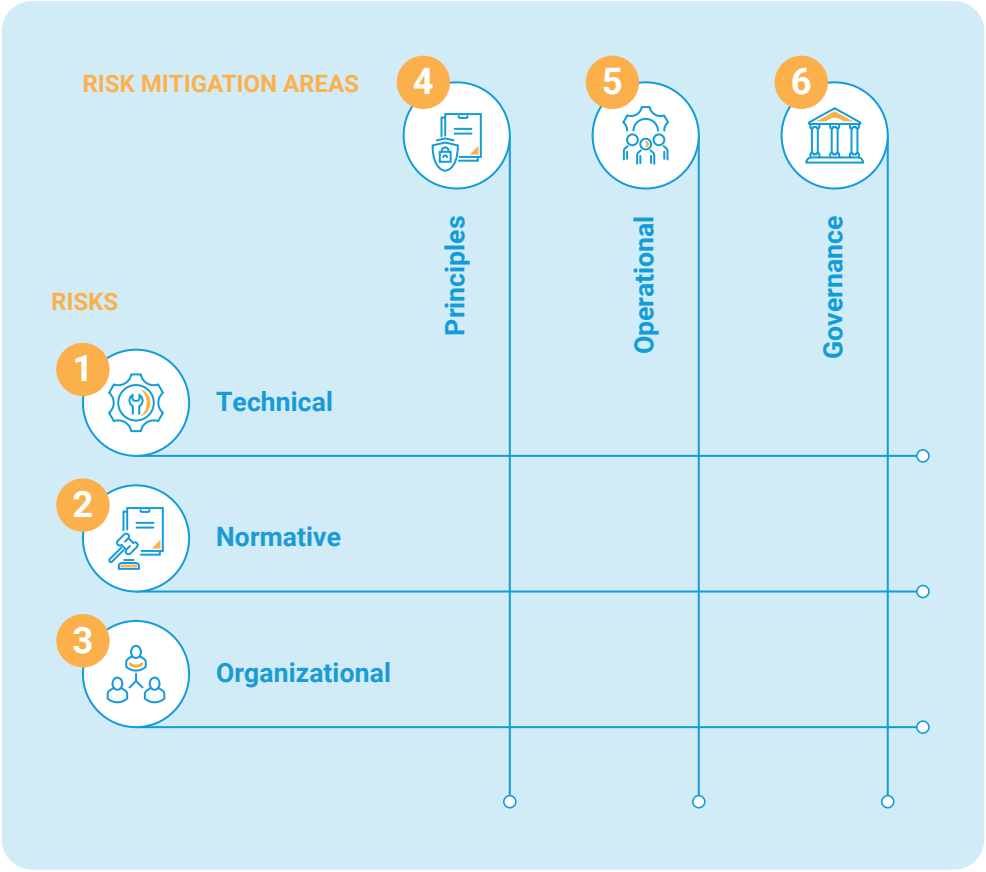
Annex 6

Methodology and Approach to Interim Report

This initiative is dedicated to building a robust DPI Safeguards framework through collaborative multi-stakeholder engagement. It is designed to respect, listen to and learn from their input and experiences. Stewarded by the United Nations, the initiative is an open space for collaboration around the development of a safe and inclusive society by leveraging DPI.

The Working Groups: A collaborative approach: The DPI Safeguards initiative involves the participation of six Working Groups. Each group is dedicated to one of the six key focus areas: principles, operationalization, governance, technical aspects, normative frameworks, and organizational structures, with continuous cross-validation. The designated Working Groups operate in a multi-phase approach: Inductive —> Deductive.

The Intersectionality of Working Groups



Inductive phase: During this discovery phase, each group systematically mapped existing definitions and best practices related to DPI safety and inclusivity within their specific area of focus. This phase involved conducting comprehensive reviews and soliciting feedback from a broad spectrum of experiences. The objective was to gain an understanding of the current landscape, study effective practices, and gather valuable insights from real-world DPI implementations.

Deductive phase: In this phase, the Working Groups transition from discovery in specific country and sectoral contexts to universalization and replicability. Here, the focus shifts to establishing context-oriented, comprehensive guidelines that address safety and inclusivity issues relevant to their respective areas. These guidelines are intended to serve as foundational elements of the framework, providing strategic, high-level direction for subsequent phases. The discoveries and insights gathered during the inductive phase translate into replicable standards and guidelines that can be universally applied, ensuring a consistent and effective approach across all areas of the framework.

The Working Groups carried out the following tasks for the Interim Report:

Research and analysis: They conducted extensive research and information gathering. They investigated relevant topics, studied best practices, conducted expert interviews, and collected data to inform the development of the framework.

Consolidation and formalization: During this phase, the information and insights gathered were consolidated into a coherent report, referred to as Deliverable 1. Working Groups transformed these insights into a structured format that aligns with the core principles of their investigative domain.

Cross-validation and reporting: Working Groups collaboratively reviewed and validated their findings to ensure their robustness and applicability. The findings were revised as needed, providing updated findings for the creation of Interim Reports.

Bringing it all together: A consultative approach: A key component of the framework is the establishment of an inclusive and diverse mechanism to seek inputs from organizations and ecosystem stakeholders.
International Organizations Consultative Group: This group comprises entities

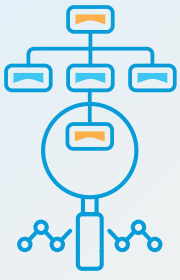
that are involved in implementing and shaping development agendas globally, regionally and locally, at a country or a state level. The Group provides valuable inputs to the different Working Groups, leveraging their expertise and experience in development, and digital transformations, and in shaping DPI approach in countries.

Multi-stakeholder convenings: To ensure varied inputs reach the Working Groups, the DPI Safeguards initiative relies on network-of-networks, including the Initiative for Digital Public Interest (IDPI), Centre for Digital Public Infrastructure (CDPI), Digital Public Goods Alliance (DPGA), Digital Impact Alliance (DIAL), GovStack, among others. The initiative has also integrated with partner organizations, in addition to global events and convenings, enabling feedback to be incorporated and recommendations to be shared through consultations.

In-country consultations: The long-term goal of the DPI Safeguards initiative is to build safe and inclusive societies everywhere across countries. Catalytic inputs will spur the necessary action for safe and inclusive implementation of DPI. To enhance the framework with a strong country-centric lens, an in-country engagement track will run concurrently.

Inputs from the ICT4D Covenings and a summary of in-country conversations were provided to the Working Groups. The Interim Report will provide an overview of the framework's components and will propose initial high-level principles.

For further details, please refer to the DPI Safeguards Initiative workbook.



- **Research and analysis**
- **Consolidation and formalization**
- **Cross-validation and reporting**
- **Bringing it all together: A consultative approach**
- **International Organizations Consultative Group**
- **Multi-stakeholder convenings**
- **In-country consultations**

DIGITAL PUBLIC INFRASTRUCTURE
Universal Safeguards

United Nations
Office of the Secretary-General's Envoy on Technology

UNDP