The Universal Digital Public Infrastructure Safeguards Framework

A Guide to Building Safe and Inclusive DPI for Societies

DIGITAL PUBLIC INFRASTRUCTURE
Universal Safeguards

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

UNDP

DIGITAL PUBLIC INFRASTRUCTURE
Universal Safeguards

The Universal Digital Public Infrastructure Safeguards Framework

A Guide to Building Safe and Inclusive DPI for Societies

September 2024

Contents

About this guide

This guide presents and explains how to apply the Universal Digital Public Infrastructure (DPI) Safeguards Framework, a set of actionable guidelines for DPI design and implementation that serve the public interest. The Framework (version 1.0) is an open public asset shared under the Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) licence. It comprises principles, process and practice recommendations to be employed by various responsible authorities within the DPI ecosystem to mitigate risks to safety and inclusivity. Risks are specified in relation to each stage of the DPI life cycle and are also addressed by upholding foundational and operational principles for safe and inclusive DPI. These principles were first introduced in an Interim Report, Leveraging DPI for Safe and Inclusive Societies, released in April 2024.

The Pact for the Future and its annex, the Global Digital Compact (GDC), were adopted on September 22, 2024, at the Summit of the Future. In the Compact, Member States recognize the potential of DPI in promoting inclusive digital transformation and achieving the Sustainable Development Goals (SDGs). Accordingly, Member States recognize the role of adaptable safeguards for DPI in achieving these goals.

The Universal DPI Safeguards Framework – A Guide to Building Safe and Inclusive DPI for Societies reflects the role of DPI and its safeguards in the GDC process. It is a multi-stakeholder contribution, motivated to ensure DPI implementations mitigate risks at both the individual and societal level, advance the SDG's and foster trust and equity across all countries.

The aim of this practical guide is to equip readers and DPI practitioners with a clear understanding of how the Framework can be applied to ensure safe and inclusive adoption of DPI. To monitor progress on this journey, Annex 4 suggests Key Performance Indicators (KPIs) that can be developed and implemented by responsible authorities to assess, analyse, benchmark and review DPI.

Executive summary

The Universal DPI Safeguards Framework has been developed by the DPI Safeguards initiative, a global multi-stakeholder effort convened and supported by the Office of the UN Secretary-General's Envoy on Technology (OSET) and the United Nations Development Programme (UNDP). The initiative engaged 44 DPI experts (from the public and private sectors, civil society, development agencies, and academia), 13 organizations constituting the International Organizations Consulting Group (IOCG), 12 countries, as well as the public through 13 convenings, and received feedback from over 100 contributors.

The Framework takes into account various 'responsible authorities' in the DPI ecosystem. It is adaptable to different contexts and is applicable across the DPI life cycle. It recognizes that DPI comprises technological systems and services that operate at the intersection of individuals on one hand, and civic, public and private entities that hold social, political and economic power on the other.

Risks related to DPI therefore do not arise purely from technical shortcomings, but also from inadequacy in normative (ethical, legal and regulatory) frameworks, as well as from institutional and organizational ineffectiveness. Risks vary significantly across different DPI systems (for example payment, identity and data exchange) and country contexts; they are not evenly distributed across society, nor are they necessarily static. Potential harms can be experienced in multiple and compound ways.

The Framework is rooted in the International Human Rights framework and the goals of the global community, specifically the Sustainable Development Goals (SDGs) and the Roadmap for Digital Cooperation. It provides process and practice recommendations to address a broad spectrum of risks to individuals. These include:

- Risks to safety—which arise from privacy vulnerability, digital insecurity, physical insecurity and inadequate recourse; and
- Risks to inclusion, arising from discrimination, unequal access, disempowerment and other forms of exclusion.

The Framework also provides recommendations to address structural vulnerabilities, such as digital distrust, weak rule of law, weak institutions, technical shortcomings and unsustainability. Emphasis is placed on the importance of robust governance mechanisms, capacity-building, and the development of standardized measures to assess the impact of DPI across different contexts.

The Framework is made up of five components:

1. Risks to be mitigated:

Risk is the possibility of harm to people interacting with the DPI. Currently, the Framework describes 13 interrelated risks.

2. Principles:

Principles, currently 18, are core propositions to mitigate risk which have been derived based on the possible risks observed in the DPI ecosystem, both new risks and existing structural vulnerabilities.

3. Responsible authorities:

A functional group of stakeholders with assigned or assumed roles, responsibilities and accountability for effective implementation and evolution of DPI safeguards.

4. Life cycle stages:

DPI has 5 life cycle stages, namely: Conception and Scoping, Strategy and Design, Development, Deployment, and Operations and Maintenance.

5. Recommendations:

These include ~ 300 processes and practices to be followed.

Thus, the Framework offers multiple permutations of risks, principles, responsible authorities, life cycle stages and recommendations. It is designed as an open knowledge asset, which allows any user to query it to identify actions they need to take.

Accordingly, this guide is intended for stakeholders with facilitating roles (ranging from conceptualization and implementation to evaluation and resourcing) within DPI ecosystems. It explains how the Framework can be used by any responsible authority to promote safety and inclusivity in, and through, DPI. It does so through demonstrative walkthroughs according to the Framework's different dimensions: (1) risks, (2) principles, (3) responsible authorities, and (4) life cycle stages.

This guide also directs readers to an interactive knowledge library, which can be queried according to combinations of the four dimensions that match the circumstances and needs of the user.

As an evolving and open public asset, the Framework will be subject to continuous updates through contributions from multi-stakeholder engagement and insights gained from country-level implementations and training. The Framework's unifying and evolutionary nature provides confidence to all stakeholders that these vital foundations of the digital economy leave no one behind and play an essential role in the delivery of public services at societal scale, a fundamental feature of digital public infrastructure.

For questions or further engagement, please email: dpi-safeguards@un.org.

1 Introduction

1.1 DPI in context

The concept of DPI is extensible and evolving. Recognizing this, the Universal DPI Safeguards Framework adopts a broad description of DPI as "a set of shared digital systems that should be secure and interoperable, and can be built on open standards and specifications to deliver and provide equitable access to public and / or private services at societal scale and are governed by applicable legal frameworks and enabling rules to drive development, inclusion, innovation, trust, and competition and respect human rights and fundamental freedoms".[1]

Noting that there are multiple models of DPI, and that each country or society will develop and use shared digital systems according to its specific priorities and needs, this broad description draws on conceptions of DPI from many organizations working globally. These include, but are not limited to, G20, the Centre for Digital Public Infrastructure (CDPI), Co-Develop, the Digital Impact Alliance (DIAL), the Digital Public Goods Alliance (DPGA), GovStack, the Organisation for Economic Co-operation and Development (OECD) and the World Bank.

Given the diversity in approaches and variety of existing DPI implementations, it is crucial to develop a unified approach to safeguards that provides universal guidance while assuring context-appropriate usefulness and usability.

1.2 The DPI Safeguards initiative

The DPI Safeguards initiative was launched in September 2023 by the Office of the UN Secretary-General's Envoy on Technology (OSET) and the United Nations Development Programme (UNDP). Its focus is systems provided by, or on behalf of, government or through public–private partnerships at societal scale which serve the public interest. The initiative followed the UN Secretary-General's policy brief on the Global Digital Compact (GDC) and its call for the creation of common frameworks for DPI. The initiative acknowledges the transformative potential of DPI while recognizing the risks that arise with any society-wide digital transformation.

The DPI Safeguards initiative is an evolving multi-stakeholder effort comprising three key pillars:

1. **Universal DPI Safeguards Framework:**
   The Framework comprises guiding principles and practices for safe and inclusive DPI, covering the entire life cycle of DPI development, from conception to operations maintenance, and including monitoring and feedback. The Framework can be accessed by using the interactive knowledge library. The library allows users to generate scenarios tailored to their context and download applicable recommendations.

[1] G20 agreed description, 2023

2. **Universal DPI Safeguards Resource Hub:**
   A dynamic online platform for community engagement offering safeguards-related resources, implementation guides, and emerging insights on DPI safeguards.

3. **Country implementation:**
   Refers to active engagement of stakeholders by the initiative and the ecosystem in countries to create or strengthen multi-stakeholder holding environments that enable spaces for sharing different viewpoints, inputs, collaboration and help address challenges. This involves facilitating technical assistance, convenings and capacity development for countries, sectors and actors to generate dialogue, build consensus, and create opportunities to advance safe and inclusive implementations.

Together, these pillars support DPI implementation in a way that is not only safe, secure and inclusive, but also practical and adaptable to diverse contexts and needs.

Foundations of the initiative

The DPI Safeguards initiative is grounded in the International Human Rights Framework. This includes the Universal Declaration of Human Rights (UDHR) which serves as the foundation for international human rights law, comprising legally binding treaties. These treaties, including the International Covenant on Civil and Political Rights (ICCPR), and the International Covenant on Economic, Social and Cultural Rights (ICESCR), collectively safeguard a comprehensive range of human rights, including but not limited to civil and political liberties, economic, social and cultural rights and non-discrimination, as well as the rights of children, women, persons with disabilities and other vulnerable groups.

The DPI Safeguards initiative is also guided by the Sustainable Development Goals (SDGs) and the UN Secretary-General's Roadmap for Digital Cooperation, both aligned to the Universal Declaration on Human Rights.

Methodology

The DPI Safeguards initiative complements, unifies and builds upon relevant existing work, including but not limited to various efforts to design, implement and sustain DPI. Annex 1 provides a non-exhaustive list of these knowledge resources. To be universally applicable to all DPI and responsive to stakeholder needs, the Framework will continue to be developed through continuous feedback cycles with multi-stakeholder inputs.

Six working groups, comprising diverse experts and DPI practitioners from a broad range of stakeholders within the global digital ecosystem (Annex 2), led the development of the Framework. Insights, feedback, and recommendations from an International Organizations Consultative Group (Annex 3), as well as from convenings, country engagements and public consultations, have informed this guide. The Framework builds on an Interim Report which was issued for public comments in April 2024. The Framework refines the risks and principles raised and provides further details on actionable guidelines adaptable to all DPI.

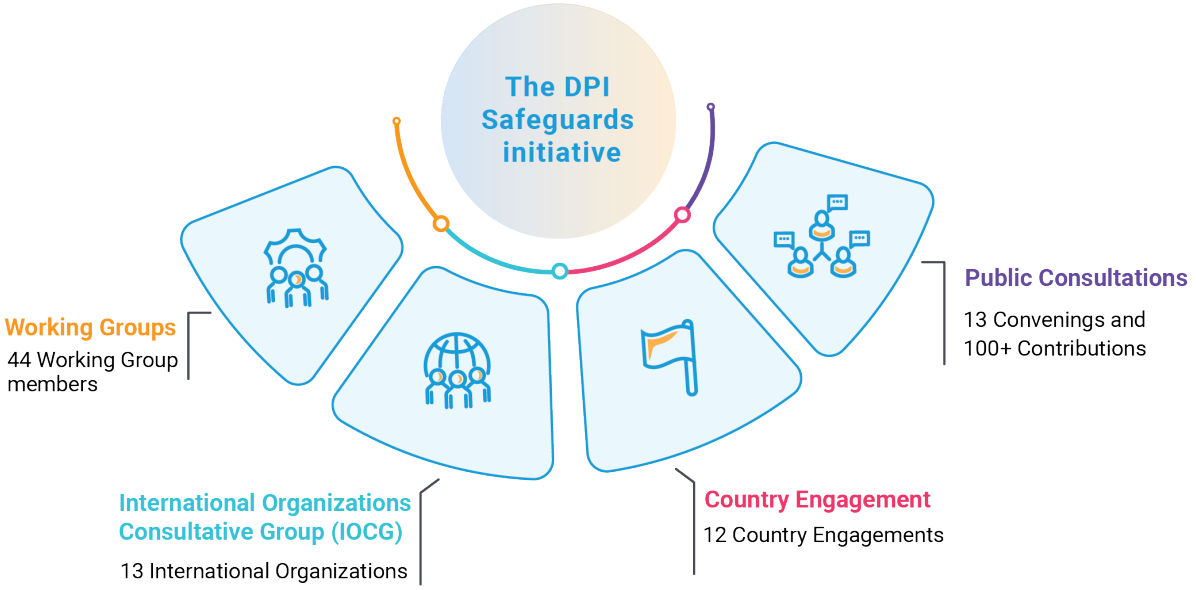

Figure 1.1 | The Framework is created through expert-led discussions and broad consultations with practitioners

2 Safety and Inclusivity for All

2.1 Why? Mitigating key risks

The impact of risks associated with DPI that is poorly designed, implemented or maintained is significant. DPI is often used to provide services by, or on behalf of, the government across society. The DPI Safeguards initiative addresses risks related to DPI that may emerge in relation to the international human rights framework, the Sustainable Development Goals, and the Roadmap for Digital Cooperation. These risks can undermine safety and inclusion and include structural vulnerabilities which limit the effectiveness of safeguards.

Risks to safety

In DPI, risks to safety arise when personal data, digital systems and the physical person or assets are susceptible to unauthorized access, cyberattacks and real-world threats. This leaves individuals and groups exposed and unprotected. A lack of or inadequate remedies and redress leaves these risks unmitigated.

The DPI Safeguards Initiative addresses the following risks to safety:

Privacy vulnerability occurs when personal information is processed (shared, stored or used) without consent, beyond reasonable privacy expectations or misused to cause harm. These breaches can lead to physical, financial, psychological, emotional and reputational damage. Notable risks include identity theft and fraud, especially in financial services such as payments and credit where victims may face severe financial losses. Privacy breaches may enable governments to unlawfully access and misuse data to infringe upon human rights through unauthorized surveillance.

Digital insecurity extends beyond privacy vulnerabilities to encompass service outages and sector-wide disruptions and other forms of systemic instability. Inadequately secured systems are susceptible to exploitation for malicious purposes, including the sabotage of critical infrastructure, unlawful surveillance, suppression of speech and assembly, espionage and the destabilization of nations. The repercussions of digital insecurity are extensive, leading to financial loss, physical danger, reputational damage and more.

Physical insecurity often stems from digital insecurity. For example, physical harm may result when medical records in a data exchange system are compromised. Intrusive surveillance may expose people's movements and places of residence to tracking, harassment or coercion. In particular, the safety of asylum seekers is threatened when their identities and movements are traceable, potentially leading to persecution, discrimination or denial of protection. Poorly secured DPI can also deny stateless persons' legal protections or access to essential services. It can be exploited to threaten the safety of individuals who express dissenting opinions or engage in lawful protest through retaliation, persecution or other forms of physical harm.

Lack of recourse refers to the absence or inadequacy of effective remedies and redress mechanisms for rights violations, leaving individuals affected by DPI risks without the means to mitigate the harms caused to them. This deficiency undermines the integrity of DPI, eroding public trust and reducing adoption rates. In turn, this challenges the sustainability of DPI, diminishes its effectiveness, and creates significant obstacles to realizing its potential benefits.

Risks to inclusion

Several risks associated with DPI could undermine inclusivity and accessibility, deterring broad engagement and minimizing benefits. While discrimination and unequal access are significant barriers, other forms of exclusion, including disempowerment, also contribute to disenfranchisement.

The DPI Safeguards Initiative addresses the following risks to inclusion:

Discrimination in any form (e.g., racial, socioeconomic, gender, disability, age, linguistic, geographic or cultural) reduces access to opportunities, economic empowerment, essential services such as health, education and participation in public and economic life. It is particularly important to avoid discrimination in digital identification (ID) systems that provide social, emergency or government services, which enable the broader economy. Discrimination is a leading cause of statelessness globally, with affected persons often excluded from ID and other systems. The digitalization of ID and other similar systems carries the risk of perpetuating existing disenfranchisement.

Unequal access to DPI is not only caused by discrimination but is also due to the digital divide and other sources of shortfall in infrastructure (electricity, Internet connectivity, smartphones, and computers), as well as socioeconomic barriers (poverty, general education, digital literacy), and service gaps in geographic areas, language barriers and disability. Human rights harms arise when access to public information and digital services is not possible due to unequal access to DPI and the social and economic structures they rely on.

Exclusion also occurs when enrolment in DPI systems is onerous, impossible or causes unease, particularly when it is a mandatory requirement to access public information or services. This often imposes a hidden cost on vulnerable individuals who may need to rely on others for assistance. In developing countries, where resources for support may be limited, the lack of alternative methods for accessing services is a prevalent risk. Courts may need to intervene to protect the rights of excluded individuals.

Disempowerment may be caused by DPI systems which restrict individuals' control over their personal data, threatening autonomy and human agency. The threat is exacerbated when people have little understanding of the possible use and reuse of the data, the associated impact, and how, or if, they can exercise control over it. Mandatory data provision can also erode human agency and, in some jurisdictions, violate human rights and civil liberties.

Structural vulnerabilities

A variety of structural vulnerabilities exist at the systemic level. Primary among these are digital distrust, weak rule of law, weak institutions, technical shortcomings and unsustainability.

The DPI Safeguards initiative addresses the following potential structural vulnerabilities:

Digital distrust may arise from known or perceived risks to safety and inclusion. Digital distrust is debilitating to the success of DPI and to the development and adoption of new innovations which enrich DPI. Like discrimination, distrust in DPI is often tied to pre-existing social factors that must be acknowledged and understood in order to be effectively addressed. Regardless of the reason, digital distrust presents serious risks to the legitimacy, effectiveness, adoption and sustainability of DPI systems and may extend to distrust in all digital services and government institutions in general.

Weak rule of law limits the ability of normative frameworks that prescribe legal, regulatory and ethical requirements to effectively mitigate risks. As DPI can amplify the political, social and economic power of those who control these systems, there is a risk that this concentrated power undermines the conventional institutions responsible for upholding the rule of law and escapes the essential checks and balances, potentially leading to abuses. Concentration of power in the form of monopolies may inhibit innovation, limit services and their features and leave inefficient quality of service unchecked. Inadequate accountability can lead to malicious use, harm, and circumvention of the law with relative anonymity.

Weak institutions diminish the effectiveness and legitimacy of safeguards by failing to implement necessary policies and practices. Insufficient institutional capacity, mechanisms and resources to fulfil necessary roles represent a pervasive risk to DPI, as does the absence of appropriate institutions to oversee the entire DPI life cycle. The lack of will or wherewithal to coordinate (or cooperate) between key agencies and stakeholders in the ecosystem to employ a whole-of-society approach to DPI diminishes its value and impact.

Technical shortcomings can be detrimental to DPI safeguards. Risks arise when technology systems are not designed to ensure safety, inclusivity and prevent harms. Vulnerabilities include security risks to the DPI itself and to people, for example inappropriate or inadequate design for specific groups and individuals (due to gender, age, disability, etc.), inappropriate technology choices leading to non-standard, non-interoperable or excessively costly solutions. Among other harms, technical shortcomings erode trust in DPI.

Unsustainability of DPI covers a broad spectrum, including environmental, financial, and partnership challenges. It poses significant risks to those who have invested in and rely on its services, and limits adoption by its potential users and those of other DPI. Such risks arise from inadequate value to users, inadequate design, maintenance, improvement, updates and resourcing. Financial threats include high operational and maintenance costs, hardware and software obsolescence and compromised components. Vendor lock-in limits flexibility and adaptability to new technologies, leading to long-term costs and other challenges. Additionally, without strategies to reduce carbon footprints and manage the environmental impact of discarded electrical and electronic equipment ("e-waste"), the environmental impact of DPI could jeopardize its role in advancing environmental sustainability goals—and in turn its own sustainability. The consequences of DPI unsustainability are significant due to its broad societal impact.

Figure 1.2 | Risks

2.2 Who? The DPI ecosystem

The DPI ecosystem includes public sector organizations, planners, legislators, regulators and adjudicators, industry organizations, private sector providers (of software, cybersecurity, cloud services, data and other products and services), maintainers of infrastructure, international and national standards bodies, international organizations, funders, non-profit organizations, advocacy groups, community representatives, individuals and a variety of other actors.

No single group of responsible authorities can enable, maintain or sustain DPI; its systems are only effective, safe and inclusive if the ecosystem is utilized with a whole-of-society approach.

To mitigate risks, it is essential that appropriate actors drive, implement and oversee all stages of DPI development and operation, with the institutional mechanisms and capacity to fulfil their requisite roles. For the purposes of the Framework, a sample of actors were considered who play an active role in enabling DPI-related services. Figure 2.1 shows these responsible authorities broadly categorized as government, regulators, donors, technology providers and advocates. While these are by no means exhaustive and may be classified in a number of alternative ways, they provide a representative sample of the key stakeholders required for DPI safeguards.

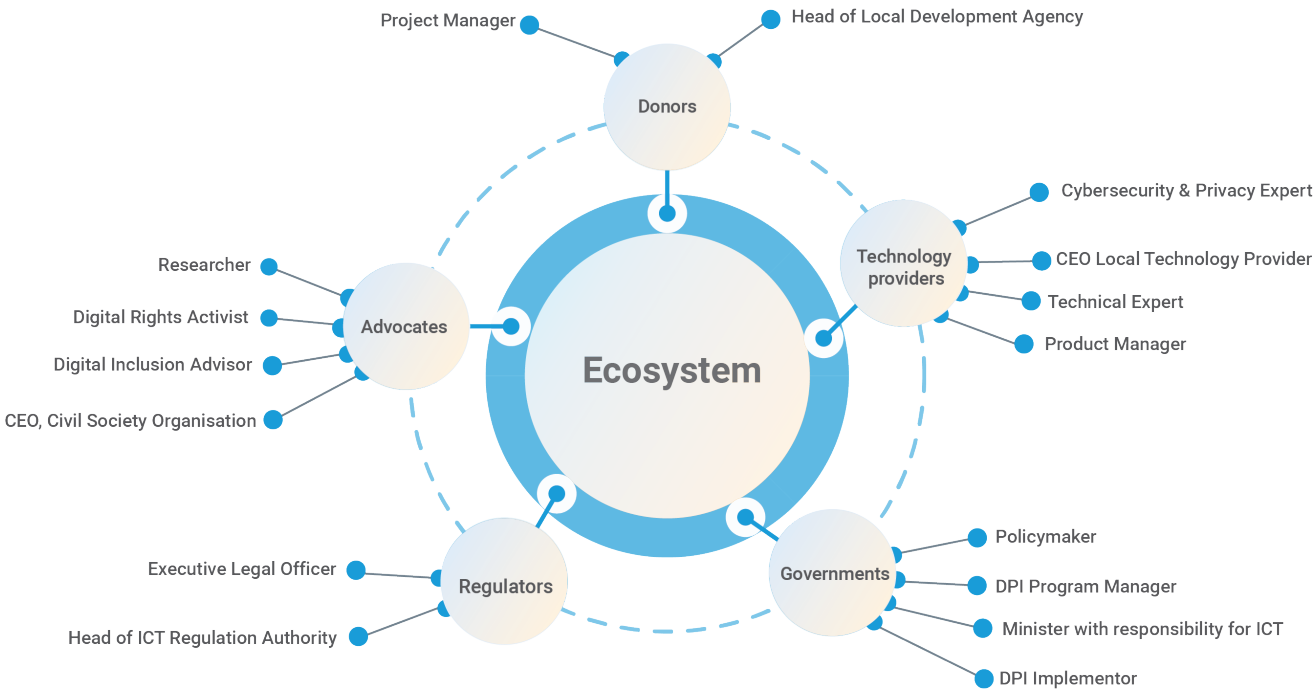

Figure 2.1 | Mapping of the DPI ecosystem

Table 2.1 is a non-exhaustive illustration of DPI-related roles held by various personae that constitute responsible authorities in the DPI ecosystem. These personae play active roles, have responsibilities and hold accountability for DPI-related services and the effective implementation of the Framework. They each have specific goals, needs, motivations, frustrations and pain points which determine how and why the Framework might be important to, and used by, them.

Table 2.1 | Possible roles and use-cases within the Framework

Responsible authority	Typical persona (non-exhaustive)	Typical DPI-related roles and responsibilities	Potential use of the Framework
Governments	Policymaker DPI Programme Manager DPI Implementer Minister with Responsibility for ICT	• Overall governance: from policy making to public service delivery • Policies to set dev. goals, guide inclusive digitalization • Budgetary support for dev. purposes and DPI development • Provide proof of progress to constituents • Listen to feedback and improve legislative, executive and judicial administration	Adopt the Framework to • Build a safe and inclusive society • Be proactive and respond to people's needs • Develop risk mitigation mechanisms • Assess current state and identify steps to be taken • Drive safe and inclusive progress towards the SDGs
Regulators	Executive Legal Officer Head of ICT Regulation Authority	• Set appropriate and effective guardrails • Supervise and enforce laws and regulations	Promote DPI safeguards in: • Frameworks and programmes for universal services • Obligation and application of concessions • Competition rules • Public relations campaigns • Voluntary codes of practice
Donors	Project Manager Local Head of Development Agency	• Provide funding and financial support. • Seek proof of progress to meet development outcome.	Add DPI safeguards to funding criteria to support and show commitment to rights-based, safe and inclusive progress through DPI to attain specific SDG-related outcomes

Responsible authority	Typical persona (non-exhaustive)	Typical DPI-related roles and responsibilities	Potential use of the Framework
Technology Providers	Cybersecurity and Privacy Expert	• Focal point for technical work, risk identification and mitigation strategies. • Influence ranges from advising to actual implementation to maintenance and support of DPI.	Adopt and incorporate DPI safeguards in practice to • Build trust as advisors to the government • Ensure success and long-term adoption of DPI. • Assess progress and develop roadmap for long term evolution of DPI. • Share safety and inclusion related best practices with stakeholders. • Actively participate in and contribute expertise to DPI safeguards community.
	CEO, Local Technology Provider		
	Product Manager		
	Technical Expert		
Advocates	Digital Rights Activist	• Drive advocacy for DPI safeguards • Work to uphold human rights • Represent interests of the marginalized and diverse sections of the society. • Provide innovative ideas to make DPI more inclusive. • Highlight incongruence with existing laws and regulations.	Use the Framework to • Assess safe and inclusive practices • Share safety and inclusion related best practices with stakeholders • Curate and share unique perspectives of their local communities with the DPI safeguards community
	Digital Inclusion Advisor		
	CEO, Civil Society Organization		
	Researcher		

2.3 When? The iterative DPI life cycle

Generally, DPI does not emerge from a linear process with a distinct start point and a fixed end point. They may evolve from existing public or private digital systems. DPI continues to change through progressive iterations and can feature new solutions over time. The continued relevance and societal value of DPI relies on iterative adjustments.

For the purposes of mitigating the risks outlined above, safeguards should be introduced during the process of DPI evolution and iteration at various stages of a typical DPI life cycle, as depicted in **figure 2.2.** These may include:

- Conception and Scoping
- Strategy and Design
- Development
- Deployment
- Operations and Maintenance

Some activities, such as learning from successful DPI models and best practices, are common across all life cycle stages. Various contextual factors, including implementation maturity, determine the evolutionary pathway for a particular DPI. Other factors, such as DPI type, sector, and service, determine the priority activities appropriate for each stage of the life cycle at different periods in its evolutionary path. The typical DPI life cycle provides a useful scaffold for identifying, mitigating and managing risk.

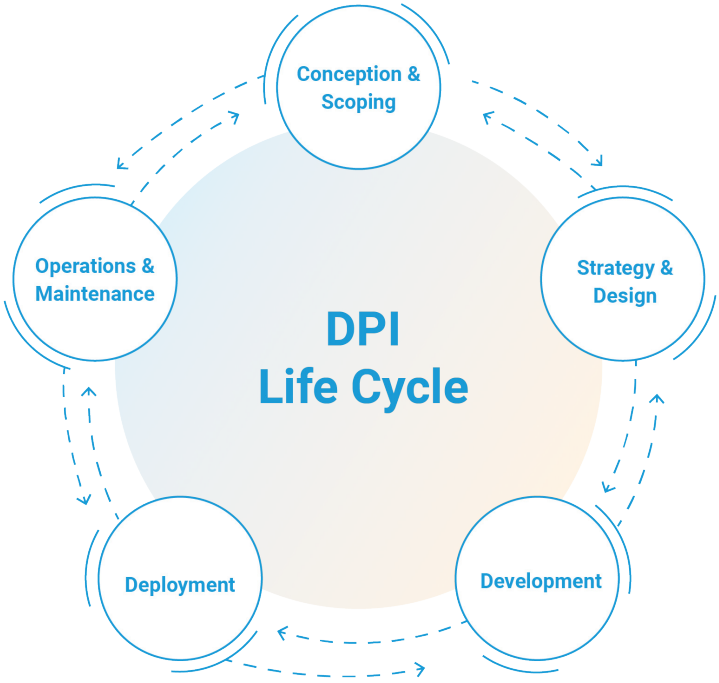

Figure 2.2 | Iterative cycles of DPI evolution

Conception and Scoping

The Conception and Scoping stage of the DPI life cycle is crucial as it establishes and reviews the purpose, goals, constraints and boundaries of a DPI. These parameters guide subsequent decision-making and ensure alignment with strategic and operational objectives, as well as the needs of individuals. Typical activities include:

- Framing of the goals and objectives.
- Identifying core problems and challenges.
- Assessing impact potential.
- Analysing the enabling environment for barriers to DPI implementation, effectiveness and adoption, taking account of relevant risks; and
- Anchoring rule of law and institutional capacity for safe, inclusive DPI implementation.

Strategy and Design

This is the stage where a comprehensive plan comprising DPI design or adjustments are formulated to translate functional and performance objectives into actionable steps, including scalability and sustainability; and planning for optimum service delivery. Typical activities include:

- Mapping and engaging with stakeholders to understand individual and societal needs.
- Identifying parties across responsible authorities and personas for collaboration.
- Raising awareness regarding the barriers to DPI implementation in the enabling environment and advocating for their removal.
- Establishing standards, protocols and metrics to assess adoption and societal impact.
- Setting design objectives and specifications according to best practices and principles with a focus on incremental improvements and resilient architecture; and employing evidence-based strategies to mitigate design-related risks.

Development

In the development stage, a prototype DPI is built according to defined specifications, ensuring functionality, reliability and scalability. Existing technical building blocks are evaluated before further development. This phase ensures that solutions are refined and tested to minimize risks and maximize the effectiveness of safeguards before widespread implementation. The mitigation of risks associated with implementation is critical at this stage, appropriate to the maturity of DPI implementation and the local context. This phase presents a valuable opportunity to empower local developers. Typical activities include:

- Evaluating and selecting existing building blocks, including technical stacks.
- Software coding to design specifications as necessary.
- Building open Application Programming Interfaces (APIs) and sandboxes.
- Analysing the enabling environment for barriers to DPI implementation, effectiveness and adoption, taking account of relevant risks; and
- Running and iterating through pilot project/s, with an emphasis on practicality and the mitigation of risks related to security, privacy, and experience of people; and
- Filling gaps in institutional structures, policies and regulations.

Deployment

During the deployment stage, the DPI is implemented in its operational environment. Any outstanding organizational changes are made to deliver value to users and to protect safety and inclusion. Change management strategies are recommended. This stage is critical to ensure successful large-scale adoption of DPI. Typical activities include:

- Installing, configuring, activating and scaling of hardware, software and networking components;
- Capacity-building of relevant responsible authorities and personas;
- Refining based on evidence, relevant data and feedback;
- Activating a robust governance framework with monitoring and redress; and
- Planned and gradual onboarding of people to carefully manage system scaling and integrity through the adoption timeframe.

Operations and Maintenance

Regular operations and maintenance ensures ongoing optimal performance, stability and efficiency of the DPI within the operational environment. Typical activities include:

- Continuous monitoring, management, maintenance, evaluation and upgrading to ensure safety and security through technical, organizational and normative means;
- Employing innovative methods for ongoing engagement across the ecosystem;
- Ensuring redressal mechanisms are fit for purpose;
- Continuously assessing readiness to leverage policy windows or opportunities to scale;
- Managing environmental impact; and
- Learning and continuously improving.

There is a need for constant learning, reflection and refinement of the overall system enabled by DPI. These learnings should be cyclical and iterative, with re-scoping when required. Moving from one stage to the next within the life cycle is determined by certain conditions. The DPI journey introduces new capabilities in stages while continually ensuring safety and inclusion. This process iterates as more use cases emerge, ensuring that the DPI continues to serve the public interest and that the evolution and effectiveness of governance keeps pace with adoption across society.

2.4 How? The harmonizing principles

Principles are core propositions that form the foundation of a flexible, universal framework that guides the effective functioning of a DPI. The purpose of DPI is to maximize participation, agency and trust for all individuals. This implies that the risks described in the sections above need to be mitigated, and residual risks need to be managed in the context of each country's sociopolitical environment. To achieve this, all responsible authorities (see table 2.1) should be guided by a set of principles to ensure trust and coordinated responses throughout the DPI life cycle. These principles form a common language that helps to build mutual understanding and support ongoing cooperation.

The principles listed in the Framework are shaped by various research methods, including consultations with diverse stakeholders, a review of secondary resources, case study analysis and discussions with country-based implementers. As the DPI landscape evolves, these principles should be periodically reviewed and updated.

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

Foundational principles: The building blocks for safe and inclusive DPI

F1. Do no harm

Harms to individuals may not be immediately obvious. A human rights-based framework should be integrated throughout the DPI life cycle to anticipate, assess, and effectively mitigate any potential human rights harms and power differentials.

F2. Do not discriminate

All individuals, regardless of intersecting identities, should have unbiased access and equal opportunity. Risks due to the circumstances of all vulnerable communities, historically marginalized groups and those who opt-out should be mitigated.

F3. Do not exclude

All individuals should have a choice of channels (digital/non-digital) to access and benefit from services enabled by DPI based on their individual capacity and resources. Access should not be limiting, conditional or mandatory — *explicitly or in practice*.

F4. Reinforce transparency and accountability

DPI should be developed with democratic participation, have public oversight, promote fair market competition and avoid vendor lock-in. All partnerships should be transparent, accountable and publicly governed.

F5. Uphold the rule of law

DPI should be introduced with a clear legal basis, with required legal and regulatory aspects embedded into its design, supported with capacity for sector specific tailoring (such as health), implementation, oversight and regulation by law.

F6. Promote autonomy and agency

Ensure that everyone (especially indigenous communities with sui generis rights), on their own or with assistance, can take control of their data, promote their agency, exercise choice, and contribute to their society's well-being.

F7. Foster community engagement

All stages of the DPI life cycle should centre on the needs and interests of individuals and communities at risk. They should participate at critical junctures and provide feedback actively in an environment of transparency and trust.

F8. Ensure effective remedy and redress

Complaint response and redress mechanisms, avenues for appeal without reprisal, supported by robust administrative and judicial review, should be accessible to all in a transparent and equitable manner during service delivery.

F9. Focus on future sustainability

Inculcating foresight is key to anticipating and limiting long term and inter-generational harms. For example, mitigating the environmental impact with a net-zero strategy or minimizing resource needs with reuse of software.

1. **Do no harm**
2. **Do not discriminate**
3. **Do not exclude**
4. **Reinforce transparency and accountability**
5. **Uphold the rule of law**
6. **Promote autonomy and agency**
7. **Foster community engagement**
8. **Ensure effective remedy and redress**
9. **Focus on future sustainability**

Figure 2.3 | Foundational principles

Operational principles: Driving continuous trust and adaptation

O1. Leverage market dynamics

DPI should foster an increasingly inclusive environment for public and private innovation such that market players can compete and introduce diverse equitable solutions that cater to emerging needs of all people across the society.

O2. Evolve with evidence

Independent, transparent, and continuous assessments, due diligence, or audits should engage with people, understand concerns, review evidence and rapidly cease or initiate activities that contain heightened risks or harms.

O3. Ensure data privacy by design

DPI should embed legal, regulatory and technical principles that enforce core privacy principles (e.g., data minimization, provisions to delink, ability to limit observability) and legal safeguards should be enacted around them.

O4. Assure data security by design

DPI should incorporate and continually upgrade security measures, such as encryption or pseudonymization, to protect personal data. A legal framework should fill the gaps where technical design may be insufficient for data security.

O5. Ensure data protection during use

Personal data should be processed or retained lawfully and transparently only by authorized personnel within a legal framework including transaction history, data subject rights and protections against overreaching requests.

O6. Respond to gender, ability or age

Not all individuals experience DPI in the same way, and some continue to face barriers and challenges related to access or use. DPI implementation should not exacerbate existing challenges or introduce new barriers and inequalities.

O7. Practise inclusive governance

Long-term effectiveness of DPI is contingent upon the establishment of a robust legal, regulatory and institutional framework that should promote transparent and participatory multi-stakeholder governance focused on safety and inclusion.

O8. Sustain financial viability

As DPI are a public infrastructure, diversified, phased and sustainable financing models should be established. Governments can lead during the build phase and local digital partners or the private sector can lead on operations and maintenance.

O9. Build and share open assets

DPI should share and reuse open protocols, specifications, Digital Public Goods (DPGs), and the associated knowledge. This enhances flexibility and assures that proprietary systems do not limit the ability to improve safety and inclusion.

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**

Figure 2.4 | Operational principles

These principles should integrate with various stages of the DPI life cycle, otherwise they risk remaining as philosophical statements. The Framework translates these principles into processes and illustrates them with observed practices so that they can be contextualized and implemented by the responsible authorities.

3 What? An Actionable Framework

3.1 The Universal DPI Safeguards Framework

The Framework translates principles into actionable recommendations, and it is agnostic in terms of its approach and definition. It is designed to be a common starting point for considering risks in countries and mitigating these risks across the life cycle of any DPI. This may range from identity or social protection systems, access to justice and health workflows, or interactions between identity, payments and case management registries or other possible combinations.

The Framework is designed to evolve and adapt to different societal contexts. As an open public asset, contributions are welcome from all stakeholders. The Framework is not a static set of guidelines, but a living body of knowledge that grows with active collaboration. Further details about the collaborative aspect of the Framework can be found in Section 4.

The five components of the Framework are described below:

1. **Risks to be mitigated (Section 2.1):**
   Risk is the possibility of harm to people interacting with the DPI.

2. **Responsible authorities (Section 2.2):**
   A functional group of stakeholders with assigned or assumed roles, responsibilities and accountability for effective implementation and evolution of DPI safeguards.

3. **Life cycle stages (Section 2.3):**
   A life cycle is composed of distinct work stages. In the case of DPI, this includes (1) Conception and Scoping, (2) Strategy and Design, (3) Development, (4) Deployment (5) Operations and Maintenance.

4. **Principles (Section 2.4):**
   Principles are core propositions that serve as a foundation for a universal, flexible, implementable and effective framework. Based on the risk observed in the ecosystem, 18 principles were developed to mitigate them.

5. **Recommendations**
   These include processes and practices as defined below:
   a. A process is a series of activities required to produce a result which may occur once, be recurrent or periodic. In the Framework, principles are translated into processes relevant to the responsible authorities at various life cycle stages.
   b. Practices are related to processes and indicate what may or may not have been done in the past. These practices are illustrative and may be evolving; they are not necessarily best practices but can serve as a reference for developing context-specific practices.

The Framework is a knowledge structure of interrelated risks with principles identified by responsible authorities linked to life cycle stages and elaborated with processes and practices. This enables anyone to query the tool as an open knowledge base and identify actions they need to take.

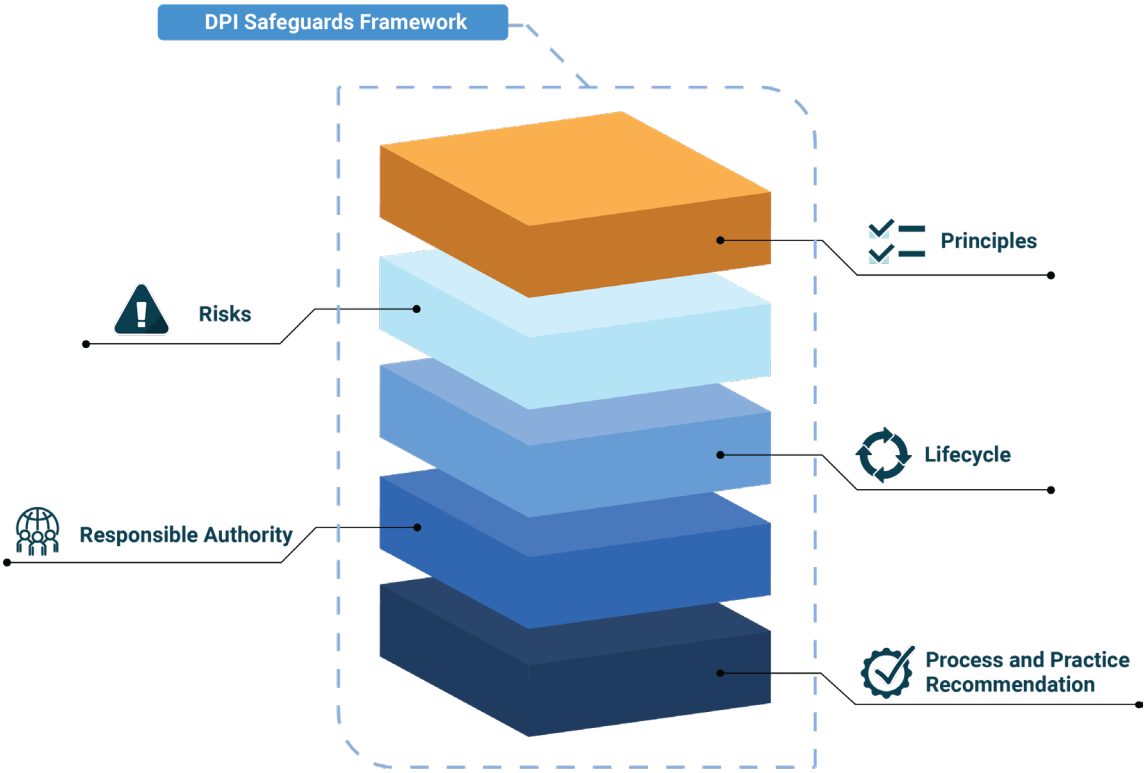

Figure 3.1 | Five components of the Framework

3.2 Navigating the Framework

The Framework can be accessed through an interactive knowledge library or the online Resource Hub. Users can access the interactive knowledge library to explore different scenarios, for example:

1. I want to address the risk of unequal access for marginalized people.
   What should I do?
2. I am a government representative conceptualizing and scoping DPI.
   Where should I start?
3. I am designing a DPI and need to address the unequal access risk.
   What should I be aware of?
4. I need to implement the principle that DPI should be non-excluding.
   Where can I find out more?
5. I want to embed privacy and data protection aspects in DPI legislation.
   What steps should I take?

6. I want to ensure effective public participation across DPI life cycle.
   Who do I need to engage with?

7. I need to design effective redressal mechanisms for DPI services.
   What do I need to consider?

Generating recommendations with the interactive knowledge library

The modular and flexible design of interactive knowledge library allows queries to generate canvases for each of the five responsible authorities, across any of the 18 foundational and operational principles, at any of the five life cycle stages to mitigate any of the 13 key risks.

The section below simulates various scenarios from the perspective of a typical user—a DPI Programme Manager—who is interested in learning about how the Framework can generate best-practice recommendations. This process can be found in the interactive knowledge library. These recommendations are provided in a format called the Universal DPI Safeguards Canvas and can be downloaded.

The following scenarios outline the needs of a Programme Manager as she explores four different scenarios and use cases

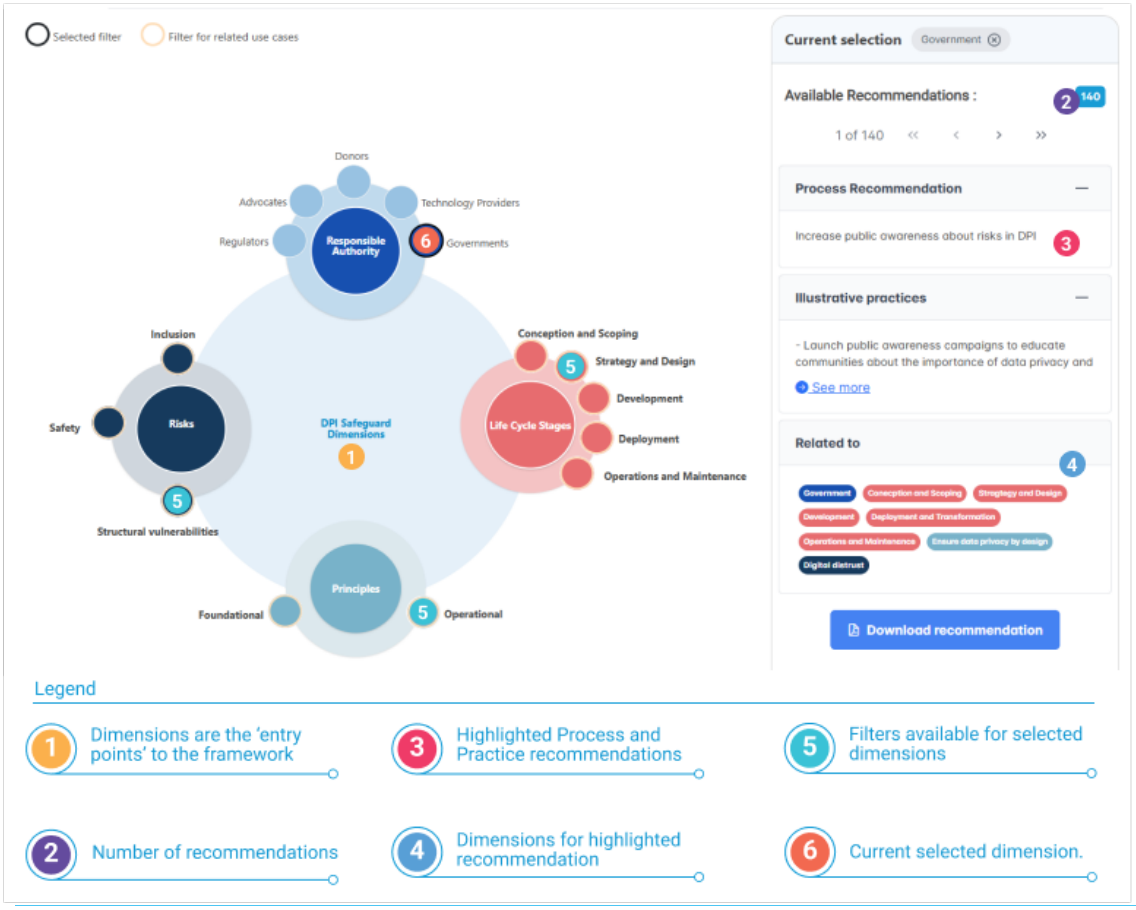

Figure 3.2 | Representation of interactive knowledge library

1. Accessing recommendations for different life cycle stages

As a government official, the Programme Manager accesses the interactive knowledge library and selects the most appropriate description of her role (her responsible authority), which is Government.

She selects the life cycle stage she is currently engaged in. As she is at the start of the process, she selects Strategy and Design as shown in Figure 3.2.

By applying these filters, the Programme Manager gains access to a set of recommendations, as depicted in **figure 3.3** below.

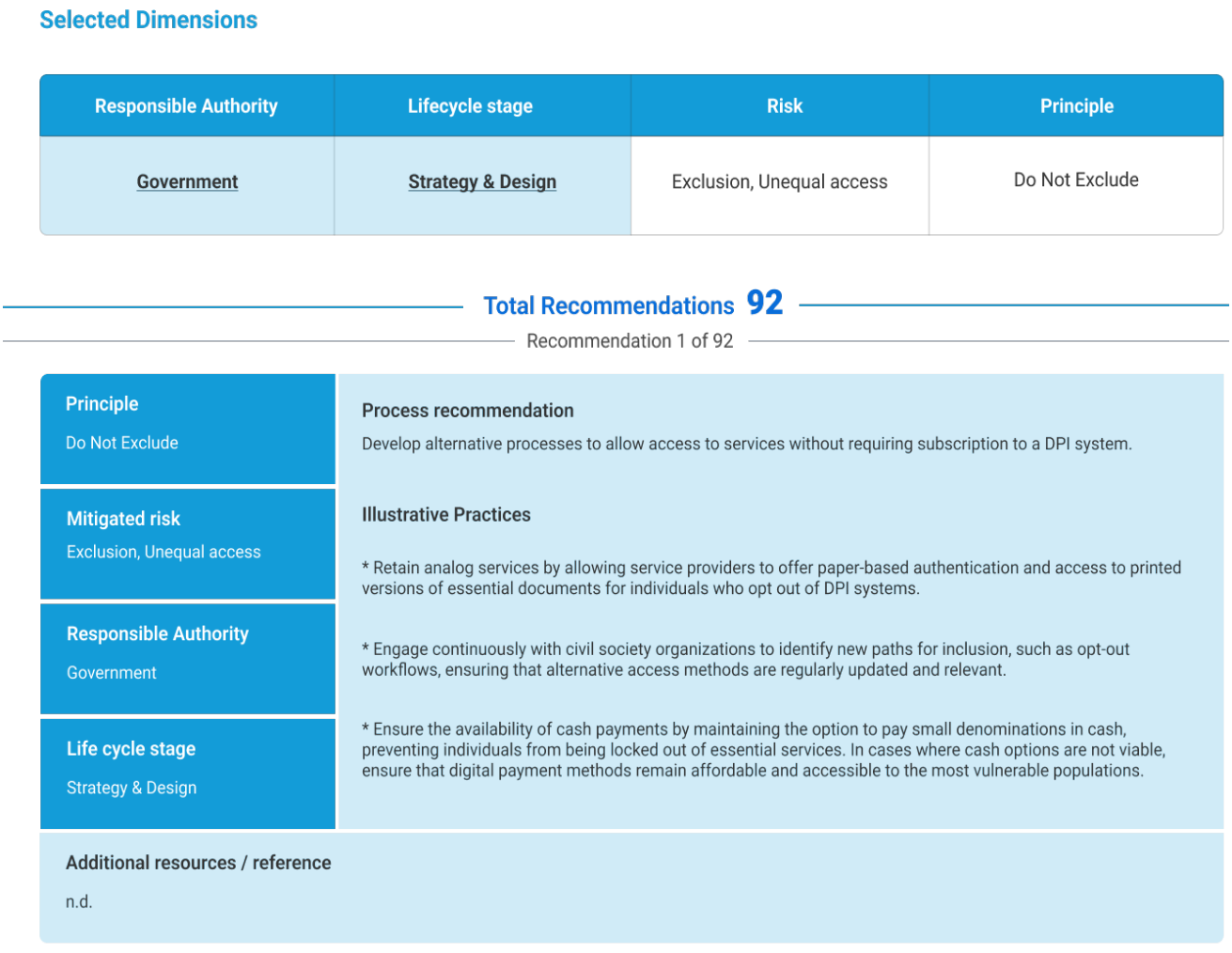

Figure 3.3 | Representation of the Universal DPI Safeguards Canvas for a DPI Programme Manager, Strategy and Design stage

Figure 3.3 shows the key principles to focus on, the processes involved, the illustrative practices that she can use and the risks to consider if she implemented these processes and practices at the strategy and design stage. This canvas is personalized, can be downloaded and serves as an easy reference for taking appropriate actions.

The content changes based on the filters selected by the user. More examples of use cases are displayed below.

The Programme Manager switches to the Development life cycle to access recommendations for this stage. The following Universal DPI Safeguards Canvas is generated:

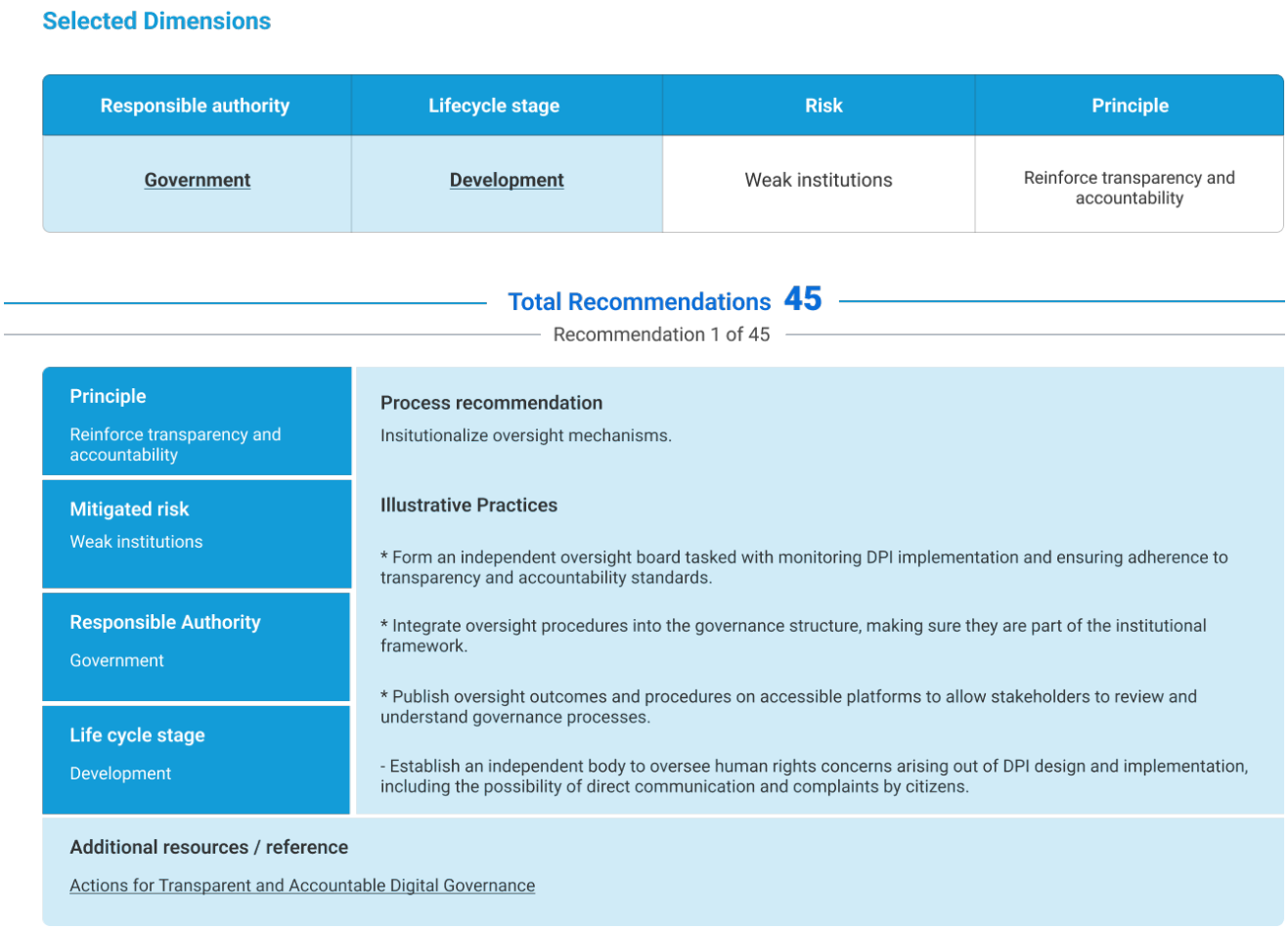

Figure 3.4 | Representation of a Universal DPI Safeguards Canvas for a DPI Programme Manager, Development stage

2. Accessing recommendations for different responsible authorities

The Programme Manager can also enter this interactive knowledge library as any other responsible authority (such as a Technology Provider) and learn what they need to do at the Conception and Scoping life cycle stage. This generates a canvas as depicted in figure 3.5. Any Technology Provider can enter the Universal DPI Safeguards Framework interactive knowledge library and see the same canvas for the Conception and Scoping stage, or any other stage relevant to them.

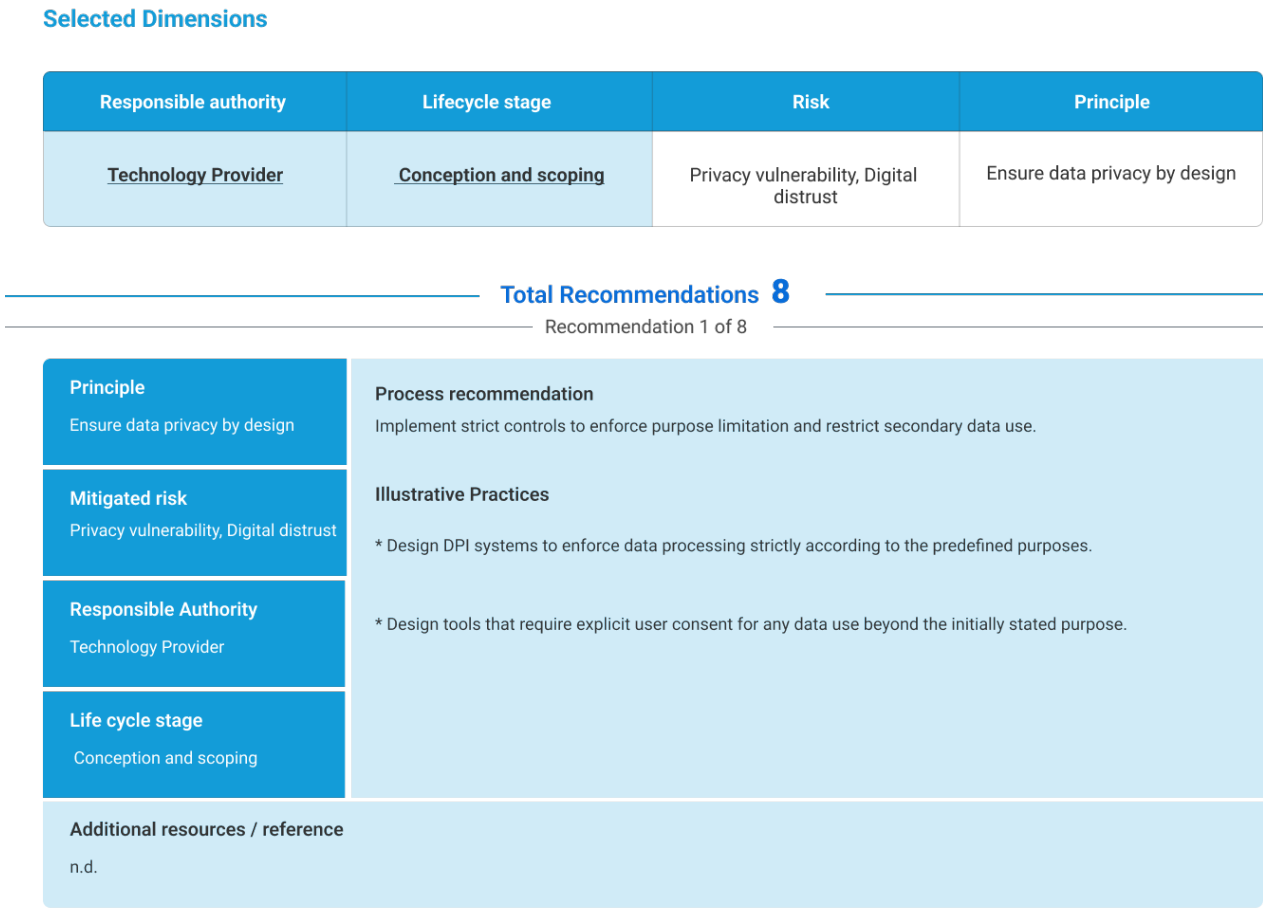

Figure 3.5 | Representation of a Universal DPI Safeguards Canvas for a Technology Provider, Conception and Scoping stage

3. Accessing recommendations by principles

The Programme Manager wants to know more about the process and practice recommendations for a specific DPI safeguards principle. She selects the foster community engagement principle (F7). This generates a canvas that highlights key processes, practices and the risks to mitigate when realizing principle F7 across the DPI life cycle. Users can repeat the same process for all the foundational and operational principles and generate recommendations for each or all life cycle stages.

Selected Dimensions

Responsible authority	Lifecycle stage	Risk	Principle
Government	Conception & Scoping Strategy & Design Development Deployment & Transformation Operations & Maintenance	Digital distrust, Lack of recourse	**Foster community engagement**

Total Recommendations 13

Recommendation 1 of 13

Principle
Foster community engagement

Mitigated risk
Digital distrust, Lack of recourse

Responsible Authority
Government

Life cycle stage
Conception & Scoping
Strategy & Design
Development
Deployment & Transformation
Operations & Maintenance

Process recommendation
Establish a mechanism for ongoing community dialogue to inform development and ensure continuous relevance.

Illustrative Practices

* Create a dedicated platform or forum for ongoing community dialogue, enabling stakeholders to regularly share feedback and insights.

* Facilitate inclusive participation by ensuring that the dialogue mechanism is accessible and represents diverse voices and perspectives from the community.

Additional resources / reference
n.d.

Figure 3.6 | Representation of a Universal DPI Safeguards Canvas for principles and recommendations

4. Accessing recommendations by life cycle stages

Finally, the Programme Manager wants to know more about the recommended processes and practices for a specific risk. She selects the risk of 'unequal access'. This generates a canvas highlighting the key principles relevant for mitigating this risk, as well as suggested processes and practices across the five DPI life cycle stages. Users can repeat this process for all risks. Multiple permutations and combinations are feasible.

Selected Dimensions

Responsible authority	Lifecycle stage	Risk	Principle
Government	Conception & Scoping Strategy & Design Development Deployment & Transformation Operations & Maintenance	**Exclusion, Unequal access**	Respond to gender, ability or age

Total Recommendations 11

Recommendation 1 of 11

Principle
Respond to gender, ability or age

Mitigated risk
Exclusion, Unequal access

Responsible Authority
Government

Life cycle stage
Conception & Scoping
Strategy & Design
Development
Deployment & Transformation
Operations & Maintenance

Process recommendation
Identify and implement additional mechanisms to always include vulnerable groups.

Illustrative Practices

* Design the system to capture and analyze data broken down by gender, age, ability, and other relevant factors to identify disparities in access and usage.

* Develop targeted features that address specific barriers faced by vulnerable groups, such as enhanced accessibility options for individuals with disabilities or simplified interfaces for older users and provide human support agents.

Additional resources / reference
n.d.

Figure 3.7 | Representation of Universal DPI Safeguards Canvas for mitigating risks

To facilitate ongoing in-country use of the Framework, any responsible authority can download a canvas using the interactive knowledge library. Release notes will be communicated to all subscribers of the Framework when it is updated with new knowledge.

3.3 Adopting the Framework

To realize the intended potential benefits of the Framework and prevent societal harms, stakeholders working on DPI implementation need to integrate the Framework recommendations into their day-to-day activities. The Framework is particularly useful when building stakeholder capacity, carrying out periodic assessments and improving governance of a DPI to proactively mitigate risks and harms.

Building capacity

Adopting the Framework involves various responsible authorities and capacity-building needs will differ across stakeholder groups. It is recommended that safeguards-related capacity-building be designed in a transparent, participatory and inclusive manner. This will ensure that all stakeholders yield significant long-term benefits across the DPI life cycle.

Community-based organizations like advocacy groups and civil society organizations help people adopt DPI-based services in a way that is inclusive and tailored to contexts of marginalized people. They advocate for these systems and provide feedback to implementation teams on the needs of historically marginalized groups. However, these organizations often lack the resources to run advocacy programmes, gather feedback, and represent communities in public consultations. This gap can be addressed through regular funding or support to build their legal and technical capacities.

DPI components and derivative systems may be developed by the private sector, local digital ecosystems and start-ups. Building their capacity is important for incorporating DPI safeguards. Responsible authorities should incorporate training and capacity-building during interagency or interdisciplinary collaborations, including during development or hiring of new staff in these areas. For judicial actors to play an effective role in the implementation of laws and regulatory frameworks, and to oversee operations in practice, capacity-building initiatives on DPI safeguards must be integrated within their professional training.

Finally, all stages of the DPI life cycle should focus on improving the capacity of people at risk. Appropriate initiatives (such as funding mechanisms, explainer series, focus groups, etc.) must be implemented to continuously educate people across diverse contexts (including language and modes of access), enable their participation at critical junctures and act on their feedback in an environment of transparency and trust.

Periodic assessments

Stakeholders need to understand the short- and long-term societal impact of a DPI. Currently there are no comprehensive tools to measure the effectiveness and impact of DPI. Impact

measurement is often viewed through the lens of legacy digital development toolkits, which place a greater emphasis on connectivity and access.

The current class of indicators is largely centred on inputs or the scale of access, with less attention given to the experience and impact on people or the DPI life cycle from design through to implementation and maintenance. Measurement methods rely on access and adoption of DPI as proxy indicators for impact and heavily use a quantitative approach. These methods, may at times, inhibit agile policy adjustments or implementations needed to drive inclusion and trust.

When first designing a DPI, it is imperative to standardize the Key Performance Indicators (KPIs) that cover the DPI life cycle and ensure these are disaggregated, analysed and reviewed by gender, age, ability and other demographic factors. Meaningful KPIs should cover five elements: 1) people, 2) institutions, 3) policies, 4) technology, and 5) innovation. Annex 4 includes checklists, questions and measurable indicators that illustrate how contextual in-country assessments can be developed and deployed by responsible authorities and key stakeholders by using assessment, analysis, benchmarking and review processes across the DPI life cycle.

Strengthening governance

Responsible authorities must develop a comprehensive outcome-oriented framework that addresses governance, oversight, and collaboration for DPI implementation across its life cycle. This framework should cover four key elements: **1) governance standards**, **2) oversight mechanisms**, **3) capacity-building**, and **4) equitable development**.

Elements	Design	Implement	Monitor
Governance standards	Develop governance standards across the DPI life cycle based on principles and processes of the Universal DPI Safeguards Framework.	Encourage adoption of these standards through updated / new policies, laws, regulations and collaborations.	Track compliance with governance standards and their effectiveness.
Oversight mechanisms	Establish shared oversight bodies.	Create standardized audit processes for DPI life cycle processes and practices.	Publish regular reports on DPI governance.
Capacity-building	Develop programmes for enhancing human capacity and civil society engagement in DPI governance.	Roll out training and awareness programmes for responsible authorities, community and the private sector.	Assess the impact of capacity-building efforts on DPI governance.
Equitable development	Create frameworks and policies for technology reuse and resource sharing between DPI.	Establish funding mechanisms for equitable DPI development.	Track reduction in digital divide and improvement in DPI sophistication.

Table 3.1 | Recommended actions to improve DPI governance

4 Evolution of the Framework

The rapidly evolving DPI landscape requires the Framework to be dynamic and adaptive. Just as the Framework has been created through an inductive–deductive co-creation process, its evolution will be guided by a continuous listening–learning updating process. This first release of the Framework (Version 1.0), lays the foundation through five components (see figure 3.1 in Section 3). It is important to note that the list of responsible authorities, practices and processes are not exhaustive, and further feedback, insights and information curated during its application will be synthesized and incorporated into the emergent knowledge base as the Framework evolves.

The Initiative will use the channels below for listening, learning and evolving the Framework:

1. **Ecosystem engagement**

   The initiative will continue to curate feedback to build additional processes and practices, KPIs and lessons learned through expert and practitioner contributions.The Initiative will continue to engage the ecosystem by creating awareness through campaigns (success stories, testimonials, and case studies), workshops and contribution calls. Public Feedback will be sought through online forums and open webinars. Special emphasis will be laid on under-represented groups. This feedback will be systematically reviewed and integrated to ensure the Framework addresses diverse perspectives and needs.

2. **Country implementation**

   The initiative will, directly and through the ecosystem, actively engage with stakeholders in countries to support their DPI adoption journeys. This will include identifying projects, facilitating connections to technical assistance/funding, and providing support for monitoring or assessment to improve impact. The experiences learned from these country implementations will inform ongoing updates and enhancements to the Framework, ensuring it remains relevant and effective across diverse contexts.

3. **International organizations**

   The initiative will continue to engage with international organizations to collaborate, advocate and support the effective use of the Universal DPI Safeguards Framework across the DPI life cycles. Feedback received from these engagements and any processes and practices used by these organization will be employed to enhance the Framework.

Regular updates will be announced and documented with detailed release notes. These updates will be openly accessible through the interactive knowledge library on the DPI Safeguards website and the DPI Safeguards Resource Hub. The updates will be available for download in multiple formats, ensuring that everyone can easily access and remain up to date on the latest version of the Framework.

Engage with us to learn more about the DPI Safeguards initiative, please visit the website and the Resource Hub to:

- Contribute to the Universal DPI Safeguards Framework
- Request advice and support for implementing the Framework
- Share general comments on the guide
- Share case studies, stories from your country, DPI or community

For any further questions or to request a customized engagement, please contact dpi-safeguards@un.org.

DPI Safeguards website	**Interactive knowledge library**	**Resource Hub**
Comments	**Contribute to the Framework**	**Request for contributions**
Workbook	**Interim report**	**Country adoption**

Annexes

Annex 1

Non-exhaustive list of knowledge resources relevant to the Framework

- United Nations Charter, United Nations (1945).
- Universal Declaration of Human Rights. United Nations (1948).
- International Covenant on Civil and Political Rights. United Nations (1966).
- International Covenant on Economic, Social and Cultural Rights. United Nations (1966).
- Sustainable Development Goals. United Nations (2015).
- Level One Project Guide. Bill and Melinda Gates Foundation (2019).
- ID4D Practitioner's Guide Version 10. World Bank, Washington, D.C., Clark, J. (2019).
- UN Secretary General's Roadmap for Digital Cooperation. United Nations (2020).
- The OECD digital government policy framework: Six dimensions of a digital government. OECD Public Governance. Policy Paper No. 02. OECD Publishing (2020).
- 10 Principles for Creating Digital Public Services. e-Estonia (2021).
- Principles on Identification for Sustainable Development: Toward the Digital Age. World Bank, Washington, D.C., (2021).
- Model Governance Framework for Digital Legal Identity. UNDP (2022).
- GovStack Implementation Playbook, GovStack (2022).
- Next Generation G2P Payments: Building Blocks of a Modern G2P Architecture. World Bank, Washington, D.C. (2022).
- Our Common Agenda Policy Brief 5: A Global Digital Compact – an Open, Free and Secure Digital Future for All. United Nations (2023).
- DPI Technology Architecture Principles. Centre for Digital Public Infrastructure (2023).
- UK digital identity and attributes trust framework. GOV.UK (2023).
- Framework for Systems of Digital Public Infrastructure (Annex 1). G20 (2023).
- The DPI Approach: A Playbook. UNDP (2023).
- Outcome Document and Chair's Summary. G20 Digital Economy Ministers Meeting (2023).
- Policy Recommendations for Advancing Financial Inclusion and Productivity Gains through Digital Public Infrastructure. Global Partnership for Financial Inclusion. G20 (2023).
- Leveraging Digital Public Infrastructure for Safe and Inclusive Societies: Interim Report. UNDP and UN Office of the Secretary-General's Envoy on Technology (2024).
- UN Principles for Responsible Digital Payments. Better Than Cash Alliance (2024).
- Outcomes of the Industry, Technology and Digital Ministerial Meeting. G7 (2024).
- ASEAN Singapore Declaration. ASEAN (2024).
- Principles for Digital Development. Principles for Digital Development (2024).

A comprehensive list of resources and reading material curated and referenced by the six working groups of the initiative are appended as Annex 1 (page 52) of the Interim Report: Leveraging Digital Public Infrastructure for Safe and Inclusive Societies, published by UNDP and UN Office of the Secretary-General's Envoy on Technology.

Annex 2

Universal DPI Safeguards working group members

The experience and expertise of the Universal DPI Safeguards' working group members engaged with the initiative ranges 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 committed volunteers, focused on developing an implementable framework for leveraging DPI to build a safer inclusive society and accelerate the achievement of the Sustainable Development Goals.

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 Organizations Consultative Group

The International Organizations Consultative Group comprises 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)
- UN Women
- UN Better Than Cash Alliance
- World Bank

Annex 4

Recommended key performance indicators

Below, the appended checklists, questions and measurable indicators illustrate the type of Key Performance Indicators (KPIs) that can be developed and implemented by responsible authorities to assess, analyse, benchmark and review processes and practices across the DPI life cycle to ensure and assure safety and inclusion of people.

PEOPLE	
Design	● % representation from all-of-society during design ● How many DPI are designed and developed locally? ● How many services mandate access through a DPI? ● % DPI-related services that have alternative / analogue access ● % services offering alternatives when a language is not supported
Deployment	● Number and % of people enrolled in DPI/DPI-based services ● % population with DPI access limitations. Where are they located? ● % enrolment of historically marginalized communities ● % unenrolled individuals who can access services using alternatives ● What is the geographical coverage of analogue solutions? How many are not available offline?
Operations & Maintenance	● % population accessing social services through innovations that leverage DPI ● % population accessing social benefits through innovations built on DPI

REDRESSAL	
Design	● What is the number of mechanisms available for effective and timely redressal? ● What types of redress mechanisms are available (administrative, judicial, other)?
Deployment	● How many public information campaigns and awareness sessions exist to explain redressal mechanisms? (clarity and ease, both online and offline, minority languages) ● Are timelines and the progress of requests clearly communicated?
Operations & Maintenance	● % issues with high impact / high severity. % of unresolved requests ● What is the average time to resolve complaints or requests, overall, for historically marginalized communities and for people with limited access to DPI ● % issues resolved to satisfaction / quality confirmed by people ● What is the average satisfaction with redress mechanisms? ● % compensation as compared to losses

INSTITUTIONS AND PROCESSES	
Design	● Are required institutions (associated and independent) in place? What is the level of readiness for DPI? Is a Human Rights Impact Assessment in place? ● What is the performance on indicators related to the Rule of Law? ● How are marginalized communities bridged to DPI with analogue support?
Deployment	● What is the sustainability model of the institutions? ● Are there any reports of exclusion due to the procedural obligations? ● What are the accountability and transparency measures for institutions? ● What is the institutional readiness to monitor the deployment of DPI?
Operations & Maintenance	● What are the support value-added services e.g., call centres? ● % availability and coverage of public centres for analogue support ● How many support-professionals are available per person? ● How many technical personnel are trained to offer 3-tier support on DPI? ● What is the level of compatibility / complementarity / convergence between existing regulatory approaches and instruments enabling data to flow with trust? ● Are the institutions able to incorporate feedback (feedback loops)? Number of improvements based on participatory feedback.

LAWS AND POLICIES	
Design	Does the law clearly establish: ● Services should offer alternatives when a language is not supported? ● Right to a legal identity for all including elements recorded and authority? ● Loss allocation regime for unauthorized and coerced use? ● Rules on burden of proof with legal presumption that favours victims? ● Right to legal aid in cases of denied access or fraudulent use? ● Equal right to access essential services through alternative / analog modes?
Deployment	Does the law clearly establish: ● Effective and practiced indicators of respect for the rule of law? ● Fair implementation of privacy laws, regulations, data related policies? ● Oversight institutions that ensure compliance to DPI standards? ● Who is allowed to access data? Are logs of who accessed data and why open to people? whose data has been accessed?
Operations & Maintenance	● What are the active, pending, and resolved cases pertaining to violation of rights? ● How many disputes are received and resolved pertaining to digital payment? ● How many DPI institutions comply with minimum DPI standards?

MARKET DYNAMICS	
Design	● How many use cases have been designed with private sector or CSOs? ● Are effective feedback loops designed to improve inclusion? ● Are inclusive and effective feedback loops designed to improve safety? ● DPI Data shared on open data platforms to support innovation
Deployment	● Which programs encourage innovation from private and CSO sectors?
Operations & Maintenance	● How many use cases utilize DPI in new product/service design? ● How much direct revenue generated by innovations built upon DPI? ● Number of persons employed by innovations built upon DPI ● How has DPI benefited the innovation / entrepreneurial ecosystem? ● Have DPI or related requirements hindered market access to businesses? ● What is the impact of DPI on the ratio of formal / informal economy?

TECHNOLOGY	
Design	● What technical standards and guidance is the DPI based on? ● Is the DPI interoperable with other systems in the country? ● Is technology deployed inclusive for both urban and rural dwellers? ● Does DPI rely on proprietary technologies? What is the degree of openness?
Deployment	● What is the average time of enrollment and number of enrollment issues identified? ● How is data shared between interoperable systems? ● How and where is data stored?
Operations & Maintenance	● What is the percentage of transaction failures by rural and urban dwellers? ● Is an environmental impact assessment in place?

Annex 5

Framework indexing guidelines for the Resource Hub

Explore the Universal DPI Safeguards Resource Hub, where each component of the Framework is indexed for easy navigation.

Risks

- RS1–RS4 for risks to individuals (safety)
- RI1–RI14 for risks to individuals (inclusion)
- SV1–SV5 risks to societies (structural vulnerabilities)

Life cycles

- L1 to L5

Principles

- F1–F9 for foundational principles
- O1–O9 for operational principles

Processes are further indexed as F1.1, F1.2 and so on, which are aligned to each principle. This enables users to locate relevant information and adopt appropriate actions from the Framework. This indexing is useful for identifying and referencing future changes across the different elements as they evolve.

Annex 6

The interactive knowledge library

To access the Interactive knowledge library and generate a recommendations canvas, please use the QR code below.

About DPI Safeguards

The DPI Safeguards initiative is a multi-stakeholder process bringing together diverse voices to develop a safeguards framework to guide digital public infrastructure design and implementation around the world.

Launched on 17 September 2023, the initiative represents a commitment to including and protecting everyone everywhere, while accelerating the achievement of the Sustainable Development Goals.

About the Office of the Secretary-General's Envoy on Technology (OSET)

OSET was created to champion global digital cooperation. Tasked with addressing emerging digital challenges, coordinating multi-stakeholder digital initiatives, and advising the UN leadership on technological trends, the Office plays a pivotal role in harnessing technology's potential for the Sustainable Development Goals. Emphasizing an open, inclusive approach, the Tech Envoy ensures synergy across UN entities, and serves as a primary contact for digital cooperation within the broader UN system.

Learn more at un.org/techenvoy and follow on LinkedIn or X.

About the United Nations Development Programme

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

Learn more at undp.org and follow on LinkedIn or X.

New York, NY 10017, USA

Donors

The DPI Safeguards Initiative gratefully acknowledges the financial and in-kind contributions of the following partners, without whom it would not have been able to carry out its responsibilities:

European Union
Co-Develop
Gates Foundation

DIGITAL PUBLIC INFRASTRUCTURE
Universal Safeguards

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

UNDP