ID4D
IDENTIFICATION FOR DEVELOPMENT

Guidelines for ID4D Diagnostics

WORLD BANK GROUP

Version Control

Version	Date	Comments
1.0	2014/07/01	Initial draft
1.1	2014/12/01	Revised to reflect feedback from ID4D Working Group (WG)
2.0	2015/08/10	Revised to reflect feedback from ID4D Working Group (WG)
2.1	2015/09/30	Revised to reflect feedback from ID4D Working Group (WG)
3.0	2016/12/01	First draft of revisions to v2.1
3.1	2017/05/01	Restructuring and text revisions
3.2	2017/06/30	Restructuring and text revisions
4.0	2017/11/10	Restructuring around *Principles on Identification*; separation of Guidelines from Report Outline; Rebranding of ID4D Diagnostic for first public version

Contents

Questionnaires

Tables

INTRODUCTION: ID4D Diagnostic

Motivation

Robust, inclusive and responsible identification systems are crucial tools for achieving sustainable development, including the World Bank Group's twin goals of ending extreme poverty and boosting shared prosperity. In addition to being the objective of Sustainable Development Goal (SDG) Target 16.9—to *"provide legal identity for all, including birth registration" by 2030*—identification is a key enabler for individuals to exercise their rights and for progress towards many other SDG targets, such as financial and economic inclusion, social protection, gender equality, and safe and orderly migration. For governments, identification systems play an important role in enhancing the capacity to target essential services such as cash transfers and subsidies, engage in long-term planning, provide security, and respond rapidly to emergencies. Digital identification systems in particular can strengthen how the public and private sectors deliver services and create a foundation on which to build new systems, services, and markets, including e-government, cashless payments, and the digital economy.

In order to meet their potential for facilitating sustainable development and improving public sector efficiency, however, identification systems must have high levels of coverage and inclusion within the population, be robust to fraud and error, and operate within a governance framework that protects personal data, promotes trust and accountability, and facilitates end-user control. In addition, many of the benefits of modern identification systems—including reduced transaction costs and facilitating new channels of service delivery—require some level of integration or mutual recognition between disparate elements of the identity ecosystem. In today's digital age and in the context of regional and global integration and migration, there is an increasing need for digital identification to be mutually-recognized and portable across countries, which can be facilitated through trust and standards.

Building robust, inclusive, and responsible identification systems is a multifaceted challenge that requires resources, technical capacity, and sustained leadership and coordination. In order to support countries in this endeavor, the World Bank Group (WBG) launched its cross-sectoral Identification for Development (ID4D) initiative in 2014. The three pillars of ID4D are "Thought Leadership," "Global Convening and Platforms," and "Country and Regional Engagement." ID4D is guided by senior leadership and a working group with members from multiple Global Practices and Departments. ID4D is also supported by a High Level Advisory Council comprised of global leaders in the identification space.

ID4D Country and regional engagement frequently begins with a diagnostic exercise—previously called an "Identity Management Systems Analysis (IMSA)"—of existing and planned identification systems. The ID4D Diagnostic methodology was developed in collaboration with governments and development partners, and provides a holistic approach to a country's identity ecosystem, including institutions, technology, laws, policies, and practices related to identification. It is guided by the ten *Principles on Identification for Sustainable Development*, which offer a framework for the realization of robust, inclusive, and responsible digital identification systems and have now been endorsed by more than 20 international organizations, development partners, and private sector associations. At the time of publishing, ID4D Diagnostics have been conducted in over 30 countries.

Goal

An ID4D Diagnostic involves an evaluation of a country's identity ecosystem according to international best practices and the *Principles on Identification for Sustainable Development* (see **Box 1**). The Diagnostic tool can be useful both for countries planning new identification systems, as well as those hoping to optimize existing systems (see **Table 1**). The goal of a Diagnostic is to:

1. **Understand and benchmark** current and (if relevant) planned identification systems to determine key strengths and weaknesses;
2. **Make recommendations** on how to improve the inclusivity, integrity and utility of existing and future identification systems for a variety of functions, including public administration, service delivery, financial inclusion, access to social programs, healthcare and education, gender equality, private sector services, and more; and
3. **Facilitate dialogue** with client governments—as well as other development partners—regarding efforts to improve identification systems.

Any recommendations that originate from the ID4D Diagnostic are country-specific and should be seen as a starting point for future TA and advisory work depending on context and demand from the client country. This can include more in-depth studies, costed roadmaps and strategies, other forms of technical assistance (TA), and World Bank lending projects. For example, a separate but related "IDEEA (ID Enabling Environment Assessment)" can be used to provide a deeper analysis of legal and regulatory frameworks related to identification, with a focus on inclusion, privacy, and data protection. Similarly, countries may require more extensive cost-benefit analyses or technical design support following the ID4D Diagnostic.

Table 1. Key benefits of the ID4D Diagnostic

Stakeholders	Benefits
Policy-level decision makers	• Inform decision making regarding gaps in identification systems, technological and design choices, and areas for reform with the highest impact • Optimize use of resources • Convene diverse identity stakeholders across the government
Identification agencies	• Resolve legal, institutional and technological issues and develop tools to strengthen administrative capacity • Adjudicate between diverse options for optimizing identification systems • Define technical and financial limitations and/or need for support
Service providers and other agencies	• Improve identity verification and authentication for service delivery, program administration, and development planning
World Bank Group (WBG) and other development Partners	• Support progress towards SDG 16.9 and other SDGs • Improve coordination and leverage multi-sectoral and regional expertise across WBG projects and those of other development partners • Identify options for supporting improvements to identification practices and systems

Scope

The goal of an ID4D Diagnostic is to evaluate a client's current and/or planned **identity ecosystem**, defined as the *set of identification systems and their interconnections within a country*. An **identification system** consists of *the databases, processes, technology, credentials, and legal frameworks associated with the capture, management, and use of personal data for a general or specific purpose.* Within a given country, there may be many types of identification systems provided by a variety of actors. The scope of the ID4D Diagnostic is generally limited to **government-issued or recognized** identification systems, however other systems—e.g., those provided by the private sector (e.g., bank identification systems) or donors (e.g., program-specific databases)—may be included where relevant.

In particular, the Diagnostic focuses on **foundational identification systems**: those created to provide general identification of the population for a wide variety of public and private transactions, services, and derivative identity credentials. Common types of foundational identification systems include civil registries, national IDs, and population registers. In addition, the Diagnostic also surveys **functional identification systems**—those created to manage identification for a particular service or transaction, such as voting, tax administration, social programs—and their relationships with foundational systems. ID4D is also planning to develop a series of **add-on modules** that can be integrated into the standard Diagnostic framework upon the request of operational teams or partners. These would provide a more focused analysis of the use of identification system for social protection, the financial sector, and other key areas of interest.

Mission and Output

ID4D Diagnostics are conducted upon request by a client country, often in connection with an existing TA or lending project (e.g., in Social Protection, Finance & Markets, Governance, Transport & ICT, Health, etc.). They are completed by a WBG task team comprised of staff and/or consultants working closely with the client government, and generally consist of four phases:

1. **Desk review** of background documents and identification of key questions and concerns from country counterparts regarding system design, governance, and inclusion
2. **Field mission** to conduct interviews with key stakeholders and collect data
3. **Report drafting** by the task team with input from ID4D staff and Working Group members
4. **Validation workshop** with country officials, government agencies, and the private sector to review and finalize the report

The end product of an ID4D Diagnostic is a Country Report that may be kept internal or published externally at the government's discretion. Because the Diagnostic framework is intended to be adaptable to a variety of systems and contexts, this report can take different forms. However, a generic outline might include the following:

1. **Introduction.** Motivation for the government, World Bank, and/or other actors to undertake the ID4D Diagnostic, along with relevant information regarding the population, economy, geography, conflict or other challenges, brief modern history of identification, etc.
2. **Identification Ecosystem: Assets and Gaps**
    a. *Identity Ecosystem Overview.* A big-picture overview of the country's identity ecosystem, including major assets, stakeholders, and architecture.
    b. *Foundational Systems*. A description of EACH major foundational system—including how it is structured and how it functions and operates, both internally and *vis-a-vis* institutional and individual users—and an analysis of the strengths, weaknesses, and obstacles to improvement of current and planned systems in terms of their design, and inclusion, and utility for end-users.

c. *Core Functional Systems*. A brief summary of major functional systems, their assets and gaps, and how they interact with foundational systems.

d. *Legal Framework*. An analysis—including strengths, gaps, and areas for reform—of the country's laws, codes, regulations, and practices related to the administration of identification systems; data collection, use, and protection; privacy; and accountability and oversight.

e. *Summary*. A summary of key strengths, weaknesses, and obstacles to improving existing and planned identification systems.

3. **Options and Recommendations.** Practical options and/or recommendations to make identification systems more robust, inclusive, effective, and responsible for individuals, government agencies, and third parties. This analysis should be highly context-dependent and pay particular attention to potential risks to exclusion and privacy, as well as feasibility.
4. **Conclusion.** Main takeaways and next steps.

Guidelines

The remainder of this document is divided into four parts, loosely structured around the *Principles on Identification* shown in **Box 1**. Part 1 begins with an overview of the identity ecosystem, including key assets and stakeholders. Part 2 focuses on the *inclusivity* of core identification systems, including coverage and accessibility. Part 3 covers the *design* of core systems, including the administrative structures, technology, processes, and operations that determine system robustness, security, responsiveness, and sustainability. Finally, Part 4 assesses the *governance* of identification systems, focusing on the degree to which the county's legal framework builds trust and protects user privacy and rights with regard to identification.

Box 1. Principles on Identification for Sustainable Development

INCLUSION: UNIVERSAL COVERAGE AND ACCESSIBILITY	Ensuring universal coverage for individuals from birth to death, free from discrimination. Removing barriers to access and usage and disparities in the availability of information and technology.
DESIGN: ROBUST, SECURE, RESPONSIVE, AND SUSTAINABLE	Establishing a robust—unique, secure, and accurate—identity. Creating a platform that is interoperable and responsive to the needs of various users. Using open standards and ensuring vendor and technology. Protecting user privacy and control through system design. Financial and operational sustainability without compromising.
GOVERNANCE: BUILDING TRUST BY PROTECTING PRIVACY AND USER RIGHTS	Safe guarding data privacy, security, and user rights through a comprehensive legal and regulatory framework Establishing clear institutional mandates and accountability. Enforcing legal and trust frameworks though independent oversight and adjudication of grievances.

Each section provides an overview of definitions and issues related to its topic, followed by a **questionnaire** that enumerates key data points and questions to guide task teams as they complete ID4D Diagnostics. In some sections (i.e., Parts 1 and 4), these questionnaires apply to the identity ecosystem as a whole. In other sections, (i.e., Parts 2 and 3) questionnaires should be repeated for *each* core identification system. The questionnaires are not meant to be exhaustive, but rather to serve as a starting point for data collection efforts. A Diagnostic should be tailored to fit country characteristics and the specific needs and requests of country counterparts.

These Guidelines are informed and accompanied by other ID4D resources, including:

- *ID4D Diagnostic Country Report Template*
- *IDEEA Framework*
- *Principles on Identification for Sustainable Development* [EN] [ES] [FR]
- *Digital Identity Toolkit: A Guide for Stakeholders in Africa* [EN] [FR]
- *The State of Identification in Africa: A Synthesis of ID4D Assessments* [EN]

For reference, previous Country Reports can also be found at worldbank.org/en/programs/id4d.

PART 1. Identity Ecosystem

The ID4D Diagnostic begins with an enumeration of major identity-related assets and stakeholders within a country. **Assets** are existing (and planned) identification systems, including their *databases and credentials* (i.e., identity documents, or IDs). Each of these systems is managed by an identity provider (agency or department) and interacts with a variety of **end-users**, including individuals (residents and citizens) and entities (e.g., other public agencies, private companies, and donors).

Major public identity assets typically include some combination of the following foundational systems, which may be managed by the same or different agencies:

- **Civil register (CR)**—A system for the universal, continuous, and permanent recording of life events—e.g., births, marriages, divorces, adoption, deaths, etc.—and associated data within the population. In addition to registering vital events, civil registries typically provide certificates or other credentials that serve as proof of identity (e.g., a birth certificate) or particular attributes (e.g., a marriage certificate to attest to marital status).[1]
- **Population or household registers**—A system that provides continuous recording of information on the entire population (children and adults, citizens and non-citizens) and/or households, including demographics and life-event information. Population or household registers are often designed to exchange information with national ID databases, civil registers, and other records.
- **National ID (NID)**—A system whose primary purpose is to issue identity credentials (e.g., a national ID card or unique ID) to serve as a general means of identification for official use. NIDs have typically been cards that are issued to those 16 or 18 years and older, but they may also be issued to children. A common function of NIDs has been to document or establish proof of citizenship; nationality is therefore a typical attribute in NID systems, regardless of whether credentials are issued only to citizens or to all residents.[2]

Countries also generally have a variety of government-provided **functional systems**, including voter registers and cards, social protection registers, tax databases and IDs, passports, driver's licenses, property and land registers, etc. The agencies that manage functional systems are also typically end-users of foundational systems, relying on birth certificates, national IDs, or other credentials to validate the identities of their enrollees.

In addition to identity providers, the Diagnostic should also consider various other public entities that play a **supporting or enabling role** in the identity ecosystem, including, but not limited to:

- *Ministries of Finance* and other agencies involved in budgetary allocations and/or decision-making for identity providers
- *Oversight and regulatory bodies* related to privacy and data protection and technology standards

---

1 The ID4D Diagnostic includes civil registers as these are an integral part of foundational identification systems (e.g., birth certificates are one of the most common "breeder" documents used as proof of identity for enrollment in other systems). However, there are other tools, such as the United Nations Statistics Division's *Principles and Recommendations for a Vital Statistics System* (see www.unstats.un.org/unsd/demographic/standmeth/principles) that provides more detailed recommendations for civil registration and vital statistics systems, which are beyond the scope of these Guidelines.

2 Recently, new models of national-level identification have emerged. A primary example is India's Aadhaar program, which issues biometric-based unique ID numbers (UID) to all residents of the country, including children, that can be used to digitally authenticate individuals for a variety of public and private services. Although creating a foundational identification system decoupled from nationality is not yet widespread, this model offers the potential to increase identity inclusion and utility rapidly in cases where citizenship is difficult for individuals to prove. In such cases, national status is treated as a "functional" attribute that can be layered on top of the unique identity platform provided by the foundational system. However, such models may not be feasible or desirable for all countries.

- Agencies responsible for inter-ministerial *coordination* (e.g., of ICT systems, strategic planning, etc.)

A variety of **non-governmental entities** also have a stake in the identity ecosystem, either as users of government-provided identities, as identity-providers themselves, or as supporting actors. This often includes:

- *Banks, mobile operators, and other companies* that are frequent users of government-provided identification systems to verify or authenticate their clients and may also provide their own forms of identification (e.g., bank IDs, SIM card registers, credit reports, etc.)
- *Donors and development partners* that finance identity-related projects, use government identification systems, or provide their own systems (e.g., UNHCR's PROGRES or BIMS systems to register and track refugees)
- *Civil society organizations (CSOs) and/or NGOs* that support residents in accessing or using government-provided identification systems, advocate for privacy and data protection, support the empowerment of women and other marginalized groups, etc.

The particular identity assets and stakeholders included in the ID4D Diagnostic will be highly dependent on the country context. In general, **the Diagnostic should focus on the main providers, users, and supporters of foundational identification systems, as well as core functional systems**. However, it can also include key private sector actors, donors and development partners active in the sector, and/or relevant civil society or non-governmental organizations, among others.

QUESTIONNAIRE 1. IDENTITY ECOSYSTEM

During the desk review phase, the team should **define assets and stakeholders** (e.g., as in **Table 2**) to better define the scope of the mission and identify key points of contact.

Table 2. Example of major identity assets and stakeholders

System	Providers	Users	Supporters/Enablers
Foundational • National ID • Civil Register • Population Register, etc.	e.g., • Minister of Interior • Health ministry • Local governments • Police	➢ Other government agencies ➢ Private sector ➢ Donors ➢ Individuals	Ministry of Finance Regulator/ oversight body Coordination agencies Civil society Donors
Functional • Voter list • Social benefits register • Tax ID • Passport • Driver's license • Cadastral system • Property records, etc.	e.g., • Electoral Commission • Ministry of Social Affairs • Revenue Dept. • Immigration Dept. • Transportation Dept. • Ministry of Interior		
Non-Government • Bank ID • SIM card database • Credit database • Donor databases, etc.	e.g., • Banks • Mobile operators • Credit agencies • Donors		

After identifying key stakeholders, the team should endeavor to **collect the following background information** for EACH foundational identity provider and any core functional providers:

- ➢ Annual budgets and expenditures
- ➢ Technical and functional specifications, including relevant technical standards (e.g. for data storage, data structure, biometric data format, etc.)
- ➢ Operational manuals, organizational charts, and organizational or sectoral plans or strategies for the development of foundational identification systems
- ➢ Past assessments or technical reports (e.g., CRVS assessments)
- ➢ National development plans or strategies that include references to identification and electronic governance (e-gov)
- ➢ Civil society reports that raise concerns about system design, governance, or barriers to access for certain groups (e.g., for women, minorities, non-citizens, etc.)
- ➢ Other relevant background documents

PART 2. Inclusion

In order for identification systems to promote sustainable development, they must have high levels of **coverage** and **accessibility**: *the degree to which the target population is enrolled in the identification system and has access to credentials and identification-related services*. Ideally, identification systems will have universal coverage, where all residents have access to proof of identity throughout their lifetimes typically starting with strong birth registration. In reality, however, many countries have low coverage in civil registration and other foundational identification systems, despite legal mandates that require enrollment. Where birth registration is low, this may hinder access to future types of ID that require birth certificates as proof of identity. This lack of access to identification is most likely to affect already vulnerable groups due to a variety of legal, procedural, social, economic, and technological barriers.

One important part of the ID4D Diagnostic is to benchmark coverage levels and provide recommendations for addressing key barriers to access. In the following sections, **Questionnaire 2** and **Questionnaire 3** should be completed for each foundational systems, as well as core functional systems.

Coverage

Principle 1	**Ensuring universal coverage for individuals from birth to death, free from discrimination.**

In assessing the **universality of coverage,** it is important to consider both *longitudinal coverage*—the degree to which there is continuity of coverage for an individual over their lifetime—as well as *latitudinal coverage*—the degree to which there is variation in coverage for different sections (and intersections) of the population. Indeed, the lack of identification often correlates with membership in various groups, including:

- Minors, including orphans and other vulnerable children
- Migrants, refugees, asylum seekers, and stateless persons
- Internally-displaced persons
- Women
- Poor people
- Rural dwellers
- Minority groups (e.g., ethnic, linguistic, religious, political, etc.)

In some cases, these inequities are the result of **policies that—intentionally or not—prevent certain groups from obtaining identification**. In other cases, they are due to **lack of administrative and technical capacity**, and/or the **various barriers** discussed in the section below.

QUESTIONNAIRE 2. COVERAGE

The team should collect **coverage data** for EACH foundational system, and any primary functional systems, as shown in **Table 3**.

Table 3. Coverage by system

<System>	Enrollment	Credential
Target population	[e.g., residents, citizens, newborns, 18+, etc.]	[e.g., residents, citizens, newborns, 18+, etc.]
Target population size	[#]	[#]
Mandatory?	[y/n/de facto]	[y/n/de facto and is it mandatory to carry?]
Total coverage - of which women/girls - of which living persons	[#]	[#]
Coverage of minors - of which girls	[#]	[#]
Coverage of under-5 year olds - of which girls	[#]	[#]
Coverage of non-citizens* - of which women/girls	[#]	[#]
Coverage of <other relevant group>	[#]	[#]

*Depending on the context, "non-citizens" can include legal and non-legal residents, refugees, asylum seekers, and stateless individuals; disaggregate where possible.

The team should also answer the following questions related to coverage and non-discrimination:

- *Variation:* In more detail, how does coverage for each identification system vary by group, including age, gender, geographic location, income level, language, ethnicity, etc.?
- *Discrimination:* Have there been reports of discrimination against particular groups attempting to register or access identification-related services, or reports of the identification system being used for discrimination?
- *Citizenship status:*
  - Does inclusion in certain registers or possession of certain credentials represent or confer citizenship? If so, how is nationality determined?
  - Are non-citizens included in the main identification systems or in separate registers?
  - What proof(s) of identity are required/accepted from non-citizens to access services and transactions?

Accessibility

Principle 2 **Removing barriers to access and usage and disparities in the availability of information and technology.**

Individuals may face a variety of structural barriers that often interact to reduce access to (and demand for) identification. These barriers include, but are not limited to:

- Economic: Poverty can be a major driver of low coverage when individuals face *direct* or *indirect* costs to enroll in identification systems and receive their credentials. Such costs may include fees for enrollment, bribes, and transportation costs and lost wages from having to visit government offices multiple times.
- **Legal and procedural:** In many countries, existing laws and procedures prevent or disincentivize certain groups from enrolling in identification systems and obtaining credentials. For example, birth registration laws that require marriage certificates from parents may prevent unwed parents or single mothers from registering their child, with lifelong effects. National ID systems that require enrollees to provide evidence of nationality may be unattainable for citizens that lack supporting documentation, especially birth certificates.
- **Social:** A variety of social barriers may also depress coverage in certain groups. Women, for example, may be less likely to enroll in identification systems where cultural norms prevent them from leaving the house unaccompanied, or from interacting with men outside of their families (e.g., male staff at enrollment centers). In addition, certain groups may have social stigmas or specific concerns regarding identification, biometric data collection, and/or privacy for certain groups.
- **Informational and technological:** People may fail to enroll in identification systems because of asymmetries in information or technology. With digital identification systems in particular, individuals may face barriers due to technological literacy issues, the inability to provide biometrics, and a lack of infrastructure (e.g., internet, electricity, authentication devices, etc.).

Identity providers should strive to remove these barriers in order to increase access to identification and the benefits and services it facilitates.

QUESTIONNAIRE 3. ACCESSIBILITY

The team should collect the information in **Table 4** on the main **economic barriers** that individuals face when attempting to access EACH foundational identification system:

Table 4. Economic barriers to access by system

<System>	
Direct cost of registration	[on time, late]
Direct cost of credentials	[first, replacement]
Penalties for non-compliance	[non-registration, no credential]
Average distance/travel time	[for registration, credentialing, other]
Average cost of travel to an office	[including transportation, lost wages, etc.]
Other indirect costs	[e.g., supplemental documentation, fixers, bribes, etc.]
Measures taken to address costs	[e.g., waved fees, mobile registration units, etc.

The team should also collect information on **other barriers** that **different groups** face in accessing EACH foundational identification system, along with steps taken to address them:

- What, if any, *legal, procedural, social, informational, and/or technological* barriers (see examples on previous page) do various groups in society face? Relevant groups might include, but are not limited to:
  - Women/girls
  - Transgender people
  - People in remote or difficult regions (e.g., mountainous terrain, areas with low internet/mobile coverage, conflict zone) or time periods (rainy season, winter, etc.)
  - Non-citizens, including migrants, refugees, and stateless groups
  - Minority groups (including linguistic, religious, and ethnic minorities)
  - Elderly and disabled people
  - Orphans and other vulnerable children
  - Illiterate people
- Have identity providers implemented any solutions to address barriers to access for the above groups, and to what degree have these been successful? Such measures could include:
  - Women-only registration units
  - Mobile or door-to-door services
  - Outreach and information campaigns
  - Forms in local languages or braille, multilingual personnel or staff trained to assist disabled or illiterate groups
  - Allowing non-binary gender categories and procedures for changing gender attributes
  - Alternative procedures for those unable to provide biometrics, proof of citizenship, or other supporting documents for enrollment/authentication

PART 3. Design

To maximize their potential for sustainable development, identification systems must have robust identity databases and credentials, and provide services that are trusted, integrated with other systems, and responsive to user demand. This requires sufficient administrative and technical capacity, appropriate technical design choices, and careful attention to user privacy and data protection. In order to achieve long-term utility and flexibility, systems must also be operationally, technologically, and fiscally sustainable.

These pro-developmental qualities depend largely on the institutional and technical design of identification systems, particularly (1) their **administrative arrangements,** (2) the procedures and technology for **data management**, including collection, validation, and storage, (3) the **credentials** issued and how they are used, and (4) the level and types of **integration** between disparate identification systems.

The ID4D Diagnostic collects data on these these four design elements in Questionnaires 4-7, which should be completed for each of the country's foundational systems, as well as core functional systems.

Administration

Countries vary substantially in their institutional arrangements for managing identification systems, including the levels of horizontal and **vertical** decentralization in foundational systems and the **autonomy** of identity providers:

1. **Horizontal decentralization** includes the degree to which foundational identification systems are managed by the same or separate institutions. In most countries, for example, civil registration and national ID agencies are mapped to different ministries. In a few cases, however, they are housed within the same ministry or even the same department.
2. **Vertical decentralization** is the degree to which the activities of any particular foundational identification system are concentrated in higher or lower levels of government or with non-government entities. Civil registration, for example, has typically been highly decentralized, with local offices conducting a majority of registration and certificate issuing, and in some cases also storing the main copies of these records. In comparison, national ID systems have often been more centralized, with data collected locally but then transferred to a ministry in the capital for deduplication and storage. Some countries also outsource certain aspects of identity management to third-party contractors.
3. **Autonomy** is the degree to which identity providers are institutionally autonomous from other government entities and whether they have the authority to generate and manage their own revenue. Civil registration providers are typically not autonomous, often reporting to Ministries of Local Government, Health, or Interior. And although national ID agencies have also typically been housed within Ministries of Interior or Police, there has been a growing trend towards agencies with fiscal autonomy who report directly to the executive or are governed by independent boards.

Beyond (though often correlated with) institutional frameworks, identity providers also vary in terms of their **levels of administrative, technical, and fiscal capacity**. In some cases, for example, providers lack sufficient funds to reform identification programs, adopt new technologies, or hire staff who are properly trained to administer their systems. Similarly, digitalization of identification systems may be hampered by poorly developed ICT infrastructure within the country, which can also inflate the budgets of identity providers who must pay high costs for internet connections and electricity.

Principle 7 **Financial and operational sustainability without compromising.**

The institutions selected to manage identification systems and their budgetary models have important implications for **long-term financial and operational stability**. Highly fractured identity ecosystems can create inefficiencies and spread limited budgets for identification across many ministries and departments. Autonomous agencies that generate and manage their own revenue may be better placed than agencies that depend on outside funding to weather economic and political shocks, preserving the continuity of identification programs and services. In some cases, identity providers adopt public-private partnership (PPP) models to finance identification systems, which can help overcome investment constraints.

Principle 5 **Using open standards and ensuring vendor and technology.**

In order to be efficient and flexible, identification systems should built using **open standards that ensure vendor and technology neutrality**. Oftentimes, agencies that lack sufficient staff and technical capacity outsource certain aspect of identity management or buy turn-key systems from identity solutions providers. To the extent that these use proprietary technology, this may result in **vendor-lock in with unsustainable costs** in the medium to long-term.

QUESTIONNAIRE 4. ADMINISTRATION

Teams should collect the information in **Table 5** and **Table 6** for EACH foundational identification system (and, if relevant, functional systems):

Table 5. Horizontal and vertical decentralization by system

<System>	<Provider>
Entity to which ID provider reports	[e.g., Ministry of Interior, executive, board of directors, etc.]
Created/assumed role	[year]
Credentials issued	[e.g., birth certificates, NIDs, etc.]
Number of offices by location	[e.g., central, regional, local-level, mobile, etc.]
Primary responsibilities of each office location	[e.g., central, regional, local-level, mobile, etc.]
Number of staff	[technical, administrative]
Average staff salary	[technical, administrative]
Key functions contracted out	[e.g., enrollment, systems integration, O&M, etc.]

Table 6. Autonomy and fiscal arrangements by system

<System>	<Provider>
Is the agency autonomous?	[y/n/partial]
Term of director	[years]
Appointment of director	[e.g., by minister, legislature, executive, competitive selection, etc.]
Procedure for dismissal	[e.g., by minister, legislature, executive, etc.]
Budgetary allocation	[e.g., how much and from which agency]
Own revenue	[e.g., amount, sources]
Manages own revenue?	[y/n/partial]
Other funding sources	[e.g., PPP, donors, etc.]
Annual expenditures	[with breakdown]
Planned investments	[with breakdown]

In addition, teams should collect information on the **main capacity challenges** for each provider, including those related to:

- Staffing (e.g., training and educational profiles)
- Budgets and finances
- ICT infrastructure (e.g., internet and electricity)

Data

The management of personal data—including the collection, validation, storage, and updating of identities and attributes—is a core activity of identity providers, with broad implications for overall system quality, utility, and privacy protection. Data management begins with the **enrollment** of individuals in the identification system, which typically includes two phases:

- **Registration and data-collection:** Individuals begin the enrollment process by registering with the identity provider. This typically includes completing a paper or electronic application form that records demographic and biographic attributes, providing supplementary documents to substantiate those attributes, and often providing biometric attributes such as fingerprints or iris scans.
- **Validation of identity information:** Once individuals have registered, identity providers then typically validate this information, including *verifying* the veracity of identity attributes and supporting documents, and potentially *deduplicating* the individual through biometric identification or other algorithms to ensure uniqueness.

After validation, individuals are enrolled and their identity **data are stored** in the system register, which may be a *paper-based filing system* or a *digital database.* Identity providers may then **update** or add attributes through one-off user interactions with the system (e.g., notifying a provider when changing an address), through mass updating exercises (e.g., re-enrollment to collect new biometric information from all individuals), or via integration with other databases. Management of identification systems also includes the **revocation or cancellation** of identities in instances of fraud or after a person's death.

Principle 3 **Establishing a robust—unique, secure, and accurate—identity.**

In large part, the robustness of the identification system—including the uniqueness, accuracy, and security of individual identities—depends on quality of information collected during the registration, the frequency of updating, the strength of validation processes, and the procedures for storing and managing personal data. For example, systems that rely on poor quality "breeder documents" to verify identity attributes will be less accurate; while those that do not collect sufficient biometric data may be less able to establish statistical uniqueness. Systems that are initially strong may lose robustness if the identity provider does not have a method for frequently and reliably updating identity attributes—such as address, occupation, and marital status—or cleaning the database to remove deceased persons. Weak data storage practices, such as paper registers and insufficient backup, also compromise system robustness.

Principle 4 **Creating a platform that is interoperable and responsive to the needs of various users.**

The type and robustness of data collected, as well as the method of data storage, impact an identification system's utility for **service delivery** and its potential for **integration** with other systems. Paper-based registers, for example, will have difficulty integrating or interoperating with other systems. A national ID system that is not deduplicated or updated to remove deceased citizens is suboptimal for generating an electoral roll that requires voters to be unique and alive. Similarly, banks require verification against accurate databases or credentials in order to fulfill know-your-customer (KYC) requirements.

Principle 5 **Using open standards and ensuring vendor and technology.**

The technology used for data management systems, including the devices used for enrollment and database hardware and software, affects the quality of the system, its flexibility, and its cost. In particular, systems that adopt technology with **open standards** enable market-based competition and innovation, creating opportunities for efficiency and functionality. Conversely, systems that opt for proprietary technology may

create "**vendor lock-in,**" binding identity providers to particular suppliers for the lifetime of their systems. This can increase costs and result in systems that are unable to adapt to meet policy and development objectives.

Principle 6	Protecting user privacy and control through system design.

Finally, the technology and procedures for data collection, validation, storage, and updating can either protect or infringe on user privacy. In general, systems should be designed according to the principle of **proportionality and minimal disclosure**, such that data collected is proportional to the use case, in accordance with global norms such as the OECD's Fair Information Practices. In general, systems should operate under a "**privacy by design**" principle that requires no action on the part of individuals to ensure that their data is protected from improper use. Data storage systems should also include sufficient security measures to ensure the protection of personal data from cyber attacks, theft, and misuse.

QUESTIONNAIRE 5. DATA

The team should collect the information in **Table 7** and **Table 8** for EACH foundational system and relevant functional systems. Note if **certain groups present additional or different supporting data/documents** (e.g. if women but not men are required to present marriage certificates, differences for non-citizens, or for children, etc.):

Table 7. Attributes and required documents by system

<System>	Type	Collection	Validation	Storage
Supporting documents required for enrollment	[e.g., birth or marriage certificate, old ID, letter from local official, etc.]	[e.g., presented copy kept, scanned, computer entry, digital transfer, etc.]	[e.g., none, calls or visits to issuer, digital verification, etc.]	[e.g., none, paper records, PDFs, etc.]
Biographic attributes captured	[e.g., name, date of birth, address, sex, etc.]	[e.g., paper form, digital scan, computer entry, etc.]	[e.g., supporting documents, calls or visits to issuer, introducer, other]	[e.g., paper records, digital database]
Biometric attributes captured	[e.g., fingerprints, iris, photo, etc.]	[e.g., inked/digital, flat/rolled, individually/4:4:2, etc.]	[e.g., none, AFIS, ABIS]	[e.g., paper copies, digital images, digital templates, whether encrypted]
Metadata captured	[e.g., time and date, geolocation, etc.]	[e.g., during enrollment, during transactions, etc.]	N/A	[e.g., paper records, digital database]

Table 8. Data storage and transfer by system

<System>	
Database architecture and location	[paper registers stored locally, centralized database in capital city, distributed databases, other]
Data transfer for validation	[paper-copies, CD, USB, internet connection, other]
Frequency of data transfer	[none, instant, hourly, daily, weekly, monthly, other]
Database security protocols, features	[e.g., encryption, firewalls, guards, etc.]
Backup and disaster recovery centers	[e.g., location, capacity, security, etc.]
Compliance with international standards	[e.g., ISO, ICAO, etc.]

In addition, the team should collect the following information for EACH foundational system and relevant functional systems:

- A narrative of the end-to-end process and requirements for individuals to (1) enroll and (2) update their information, including the ease or difficultly with which individuals can change certain attributes (e.g., address, sex or gender, etc.)
- The location (e.g., local, central, etc.) and responsible parties (e.g., local officials, central officials, private firms, etc.) for core activities, including enrollment, verification, deduplication, database management, updating, etc.
- The type of technology used for data collection and storage and whether open or proprietary
- Whether any sensitive personal data is collected (e.g., on race, ethnicity, religion, etc.) and what, if any, additional security measures are taken to protect these attributes
- Statistics on false rejection, acceptance rates (FRR and FAR) for biometric enrollment, if available
- Policies/procedures for invalidating or cancelling identities in the case of theft, fraud and/or death
- History of issues with the loss of records, database breaches, etc.

Credentials

In order for individuals and other end-users to take advantage of identification systems, they need **credentials**: *mechanisms, processes, devices or documents that vouch for the identity of a person through some method of trust and authentication.* Credentials allow a person to prove who they are (authenticate) and verify particular attributes of their identity (e.g., age, address, enrollment in a social security program, etc.). The nature of the credentials issued and how they are used vary substantially across identification systems and countries, including:

- **Types of credentials issued:** For most foundational and functional systems, common credentials include—but are not limited to—cards, booklets, numbers, mobile IDs, and certificates. Credentials can *be analog or digital*, and vary in their *form-factor* (i.e., the material they are made from and their embedded features).
- **Information contained:** Credentials also vary in terms of the information they contain. With cards, for example, this includes identity attributes that are *human readable* (i.e., they are printed on the card) and/or *machine readable* (i.e., they are stored in a barcode, chip, etc.). For ID numbers, some are *generated randomly* and contain no information, while others are sequential and may be encoded with information such as place and order of issue, gender, and residence.
- **Authentication capacity:** The ability to use credentials for authentication is largely a product of the type of credential and the information it contains. Digital authentication, for example, typically requires a credential such as a smartcard, mobile ID, or unique ID number (UIN) in combination with another factor (e.g., a PIN number or fingerprint). However, the implementation of digital authentication also requires ICT infrastructure, such as reliable internet connections (for authentication against a database) or a network of POS devices (for local authentication).

Principle 3 **Establishing a robust—unique, secure, and accurate—identity.**

The type of credential used and the information and features it contains have implications for its **robustness**—i.e., its susceptibility to loss, damage, theft, and tampering. Laminated ID cards, for example, are much easier to alter and fake than digital smartcards with holograms and other security features; paper certificates are similarly easy to damage or forge. Cards may be easier to fake or lose than ID numbers, while ID numbers may be more easily forgotten by users, particularly those who are illiterate. In addition, credentials that offer the potential for multi-factor digital authentication can enable higher levels of security for transactions, reducing the likelihood of identity fraud.

Principle 4 **Creating a platform that is interoperable and responsive to the needs of various users.**

As with data management, the type, information, and authentication capacity of a credential impact an identification system's utility for **service delivery** and its potential for **integration** with other systems. For example, a bank that wants to use a national ID card to verify the signature of new clients offline will only be able to do so if the card has a picture of the individual's signature. A smartcard can only be used for international travel if it is compliant with ICAO standards for travel documents. Service providers will not be able to offer digital authentication for transactions unless the credential provides this capability.

Principle 5 **Using open standards and ensuring vendor and technology.**

Similarly, the standards and technology used for credentials and authentication mechanisms also impact system's utility and and sustainability. The use of **proprietary technology** for credentials (specifically ID cards) may increase the cost and difficulty of integration with other identification systems or service providers. Smart ID cards that use proprietary encryption technology, for example, will require POS devices

that are licensed to be able to read them. This limits the potential for competition among device providers and will likely raise the cost of extending authentication infrastructure throughout the country.

Principle 6	Protecting user privacy and control through system design.

Credential type, information, and authentication processes also have implications for individual privacy and control. As with data collection, information contained on credentials should follow the principles of **proportionality and minimal disclosure**. Credentials, including ID cards and numbers should not disclose sensitive personal information that violates individual privacy and may facilitate profiling of individuals. Authentication protocols should similarly disclose only the minimal data necessary to ensure appropriate levels of assurance, based the level of risk and international standards (e.g., those provided by NIST or eIDAS). In addition, countries should weight the benefits of multi-purpose credentials with concerns regarding over-disclosure or centralization of personal data.

QUESTIONNAIRE 6. CREDENTIALS

For EACH foundational and relevant functional systems, the study team should collect information on the **type of credentials** issued, their **form factors**, and the **information they contain**, as shown in **Table 9** (e.g., for ID cards, certificates, etc.) and **Table 10** (e.g., for ID numbers).

Table 9. Physical or soft credentials by system

<System>	
Type of credential	[e.g., card, certificate, mobile ID, token, etc.]
Date current credential began issuance	[year]
When issued and to whom	[e.g., all residents at the age of birth, adult citizens, etc.]
Expiration after time of issue	[e.g., 10 years]
Human-readable attributes visible on credential	[e.g., name, address, date of birth, signature, photo, fingerprint, ID number, expiration date, etc.]
Machine-readable attributes stored on credential	[e.g., demographic information, number of biometric images/ templates, etc.]
Material	[paper, laminated, PVC, polycarbonate (PC), mobile SIM card, other]
Machine readability	[none, mag-strip, barcode, chip (& size), RFID, other]
Encryption	[none, symmetric, PKI/digital certificate (signed by who?), encrypted fingerprint templates, other]
Security features	[none, holograms, microtext, UV, engraving, other]
Credential personalization	[local, centralized]
Timeline for issuance	[hours, days, weeks, or months]
Method of collection	[in person, mail, digital, other]
Options for requesting new and replacement credentials	[in-person, website, mobile application, other]
Compliance with international standards	[e.g., ISO/IEC 7810, ISO/IEC 7811, ISO/IEC 7816, ISO/IEC 14443, ICAO 9303, etc.]

Table 10. ID numbers by system

<System>	
Year current version of number began issuance	[date]
When issued and to whom	[e.g., to all residents at birth registration, to national ID applicants, etc.]
Expiration after time of issue	[e.g., never expires, used for lifetime; when applying for a new ID card, etc.]
Type and format of number	[e.g., 10 digits random with 2 check-sum digits, 12 digits structured]
Numbers of deceased individuals are recycled?	[y/n]
Number printed on birth certificates?	[y/n]
Number based on biometric deduplication?	[y/n]
Compliance with international standards	[e.g., ISO, ICAO, etc.]

In addition, the team should collect the following data for each assessed credential:

- A narrative of end-to-end process of credentialing, including the *location* (e.g., local, central, etc.) and *responsible parties* (e.g., local official, private company, etc.) for core activities including personalization, distribution, etc.
- The type of technology used for credentials and whether open or proprietary.
- Whether and how each credential is being used by individuals for *verification* and/or *authentication* including:
  - Offline and online processes and devices
  - Types of factors used and whether these vary based on application
  - Which service providers or entities are included in the authentication infrastructure
  - Alternative or secondary procedures for authentication in case of failures
- Frequency of types of fraud involving the credential—for example, whether it is easily or commonly faked, stolen, or manipulated.
- Processes for deactivating credentials compromised by fraud or after the death of the owner.

Integration and Applications

Broadly speaking, an identification system's level of **integration** is the degree to which it is **linked** to other systems within the country or across borders. There are various types of linkages that may increase integration, including:

- **Interoperability between databases**, or the degree to which separate systems can talk with each other, exchanging information or receiving responses to queries. In some cases, databases may be *directly connected*, allowing for the real-time exchange of information. In other cases, multiple databases may be *indirectly interoperable* via a trust framework that allows for communication and queries.
- **Online interfaces** such as *application program interfaces (APIs)* can also facilitate integration by allowing users from one institution limited access to query the database of another institution as needed (e.g., allowing banks to query NID providers in order to fulfill KYC requirements for a new account holder).
- **Common identifiers** such as UINs or ID cards can also link two systems together. In digital systems, they are often used as keys to facilitate interoperability or online queries. However, the use of common identifiers in non-networked systems can also create dependencies that streamline identity management. For example, a paper-based system where all service providers use the national ID card for identity verification is more integrated than one where each service provider issues its own card.

In general, **fragmented identity ecosystems**—those with low levels of integration—are inefficient. Each agency or department conducts separate registration exercises (e.g., for the national ID, voter lists, social programs, health insurance, etc.) collecting and managing many of the same attributes in parallel systems. Without the exchange or verification of information across databases, each agency must undertake its own labor-intensive and duplicative exercises to validate the identity attributes it collects.

The level to which an identification system is integrated with other institutions therefore affects the robustness, utility, and financial sustainability of the system. This is particularly the case with **integration between national ID and civil registration systems**, which should be a key focus of the ID4D Diagnostic. In addition, policies and protocols for data sharing and access have important implications for the protection of personal data and privacy.

Principle 3	**Establishing a robust—unique, secure, and accurate—identity.**

Integration between identification systems can be crucial for **robustness**. In order to maintain the accuracy of identity information, systems need to be continuously updated to reflect changes in identity attributes. Voter registers, for example, need current information on age, address, and whether or not previously registered voters have died. Rather than updating each database through independent data collection efforts, interoperability—particularly with civil and population registers that track vital events—can simplify data management.

Principle 4	**Creating a platform that is interoperable and responsive to the needs of various users.**

Interoperability and other types of linkages help **stimulate demand** for identification and authentication services, increasing coverage and utility for a variety of users, including other government agencies, private companies, and individuals. Individuals, for example, are more likely to want to enroll in identification systems that provide access to a wide variety of services. In fragmented ecosystems, the need to spend time and resources to register separately for each identification program (and carry multiple ID cards) may overburden users and deter them from accessing systems.

Principle 7 **Financial and operational sustainability without compromising.**

Increasing the integration of identification systems can also facilitate **savings** for governments by decreasing redundancies within the system and lessening administrative burdens related to identity verification and authentication. With high levels of integration, for example, countries may be able to **eliminate duplicative data collection**, and some legacy systems and credentials may even become obsolete. Furthermore, the incorporation of a foundational unique ID into functional systems can deduplicate program databases and eliminate multiple or fake enrollments, potentially **reducing leakage** in payroll and social programs. Integration between various functional databases (e.g., cash transfer, tax, and property databases) can help identify discrepancies and fraud. Finally, where foundational identity providers offer online linkages with third parties (e.g., banks, other agencies), they can **generate revenue** by charging for digital authentication and verification services.

Principle 6 **Protecting user privacy and control through system design.**

Despite these benefits, however, integration can create challenges for user privacy and data protection. For example, a fully centralized and integrated system with a single data warehouse would present **security challenges** and may infringe on the principle of **proportionality and minimal disclosure** if all agencies using the database have access to all identity information. Instead, interoperability and sharing between databases should follow international standards for security and encryption, proportionality and minimal disclosure. For example, many countries have established elaborate mechanisms to ensure that each agency only has access to a minimum amount of data common to all databases. This may include the national ID number as well as some additional variables, such as date of birth and sex. Program-specific information, such as employment histories, medical records, and other sensitive data, remains accessible only to the relevant agency. These issues are particularly relevant in countries that do not yet have adequate legal frameworks for data privacy and protection.

QUESTIONNAIRE 7. INTEGRATION AND USES

The team should collect information on **interoperability** and **dependency** in **Table 11** and **Table 12** for EACH foundational system and any relevant functional systems:

Table 11. Database integration by system

<System>	
Databases with which system exchanges information	[e.g., none, civil register, population register, voter database, immigration database, vital statistics, etc.]
Data exchange technology	[none, exchange later, API, wired connection, CD, paper, other]
Frequency of data exchange	[none, live, hourly, daily, weakly, monthly, other]
ID numbers included in database	[e.g., NIN, tax ID, etc.]

Table 12. Integration for service delivery by system

Service	Dependency on <credential>	Verification of <credential>	Authentication of individual
Benefits: enrolling in or collecting G2P transfers, e.g., payroll, pensions, emergency or cash transfers, rations, energy subsidies, insurance, etc.	[required, accepted]	[none, phone, digital, other]	[none, via credential, via database, +method]
Education: primary/secondary school or university enrollment, exams, student loans, etc.			
Health: enrollment in health insurance, hospital visits, etc.			
Finance: applying for bank account or loan, credit scores, purchasing property, notaries, etc.			
Elections: registering to vote, voting, registering as a candidate, etc.			
Taxes: filing taxes, applying for a tax ID number or card, etc.			
Travel & transport: international travel, applying for a passport or driver's license, etc.			
Utilities: buying a SIM card or mobile phone, subscribing to water, gas or electic services, etc.			

In addition, the team should collect the following information on integration:

- A detailed description of integration between foundational systems—particularly between national identification or population registers and civil registers
- Detailed descriptions of authentication processes involving key foundational credentials
- An assessment of whether—and how—the current identification system is currently meeting user demands across a variety of sectors
- Whether any credentials or systems are interoperable with or recognized by identification systems in other countries.

PART 4. Governance

Identification systems must be built on a legal and operational foundation of trust and accountability between government agencies, international organizations, private sector actors and individuals. To this end, the ID4D Diagnostic includes an analysis of governance frameworks across all identification systems in **Questionnaire 8.** This includes **existing and draft country laws, codes, regulations, and agency practices** related to:

- The administration and authority of national ID agencies, civil registers, and other identity providers
- The collection, storage, and use of personal data, both analog and digital
- Conferring or proving citizenship or legal status through identification systems
- User privacy and data protection
- Accountability and oversight, both between identity providers and other government agencies, and between identity providers and users.

In some countries, legal frameworks and practices may already enable robust identification systems, while in other cases they may need to be updated to comply with international law, clarify administrative authority, incorporate new identification technologies, protect the data the privacy of individuals, and ensure the accountability of agencies that collect, store, and use personal information. In many cases, such laws and regulations do not exist, are not enforced, or predate the advent of ICT, electronic storage, retrieval and management of digital records and databases.

Principle 8	**Safe guarding data privacy, security, and user rights through a comprehensive legal and regulatory framework.**

Identification systems should be underpinned by comprehensive legal frameworks and practices that promote trust in the system while stimulating competition and investment. This includes ensuring **the protection of individual data, privacy and user rights**. Individuals should have genuine choice and control over the use of their data, including the ability to: (1) selectively disclose only those attributes required for a particular transaction, (2) easily correct inaccurate data free of charge, initially through administrative (rather than judicial) processes, and (3) obtain a copy of their personal records, as well as information on who has accessed them.

In addition, personal information should not be used for unauthorized surveillance or profiling by governments or third parties, or secondary, or used for unconnected purposes without consent (unless otherwise required under the law). Legal frameworks and policies related to data sharing and usage should be clearly and publicly documented, and be updated to reflect the digital age.

Principle 9	**Establishing clear institutional mandates and accountability.**

Creating a harmonized, robust identification system with wide coverage requires an overarching legal and procedural framework that provides transparent and comprehensive institutional mandates and accountability. The role of each identity provider should be clear and publicly available, as should responsibilities within each institution. Identity providers should establish memoranda of understanding (MOUs) with other agencies for the exchange and use of data and for authentication and verification services.

Principle 10 **Enforcing legal and trust frameworks though independent oversight and adjudication of grievances.**

Finally, countries should have independent oversight bodies for ensuring compliance with legal and policy frameworks related to the collection and management of personal data. Such entities should be empowered to ensure that identity providers adhere to their mandates and responsibilities, respond to potential data breaches, and adjudicate and redress disputes over the use of personal data that are not resolved through administrative processes.

QUESTIONNAIRE 8. GOVERNANCE

The task team should begin by listing all **ratified and draft domestic** laws and acts—as well as any **international or regional conventions** to which the government is a party—pertinent to identification, including those related to topics in **Table 13**:

Table 13. Identification-related laws

Topic	Laws/Acts/ Conventions	Enacted	Enforced	Revisions	URL
Civil registration					
National ID					
Voter registration					
Citizenship					
E-Government					
Privacy & personal data protection					
Electronic/digital signatures					
Transparency & right to information					
Equality and non-discrimination					
Other					

The team should the assess the strength of the above **legislative framework** as well as **operational policies and procedures** (e.g., as enumerated in MOUs, internal operations manuals, etc.) with regard to the following:

- **Roles and responsibilities:** The authority and role of identity providers and other actors is (1) clear, (2) comprehensive, and (3) streamlined within the legislative framework and in practice. Specifically, the degree to which:
  - The roles and responsibilities of different entities—including (a) identity providers, (b) supervising agencies, (b) other government actors, (c) private firms, and (d) individuals—and their relationships vis-à-vis each other are clear and non-conflicting
  - Independent, neutral agencies are legally empowered to monitor, oversee and/or supervise identification systems and have sufficient resources and sanctioning power to enforce the laws, ensure the accountability of identity providers, and adjudicate disputes.

- Ownership of data is clearly articulated, including whether or not the state retains ownership over data collected by private entities
- There is regulatory direction and/or a credentialing process for private firms involved in the identity ecosystem

- **Data protection and privacy:** Laws, policies, and procedures provide sufficient user privacy, control, data protection and security, and meet the standards of minimum data collection and purpose specification. Specifically, there are:
  - Explicit protocols and technological controls (e.g., privacy-enhancing technologies, or PETs) that limit how and when different government agencies and private firms can integrate or interoperate their databases and what information can be shared for identity verification and authentication
  - Mechanisms to inform individuals of their privacy rights and obtain informed consent—including for minors—on the initial collection and use of their data and renewed consent when data is used for purposes for which it was not collected
  - Clear and streamlined administrative procedures to address duplicate records, correct errors, adjudicate and address grievances, and remedy identity fraud or theft
  - User-friendly mechanisms for individuals to view their records, see who has accessed them, edit or update information, and contact data controllers to address any grievances
  - Clear, explicit, and legitimate specifications regarding the purpose of data collection, established procedures for deviating from this purpose, and fair policies regarding data retention and destruction after the purpose has been completed
  - Degrees of confidentiality and heightened security measures for certain types of data (e.g., for biometrics, sensitive data such as ethnicity and religion, or changes in sex or gender designation), or the possibility for individuals to decline to provide this data and still be enrolled
  - Clear confidentiality and anticorruption policies for staff, incentives (internal and/or external) to assure collected data is used as intended, and established procedures for addressing deviations from these policies
- **Scope:**
  - Laws governing the collection, storage, and use of personal data cover both analog and digital systems
  - Laws are compatible with relevant international and regional conventions (e.g., the 1989 Convention on the Rights of the Child (CRC)) and the government has met its obligations with regard to these conventions
  - There are sufficient legal protections against discrimination in identification systems based on race, ethnicity, religion, sex, political affiliation, etc.

worldbank.org/id4d

ID4D
IDENTIFICATION FOR DEVELOPMENT

WORLD BANK GROUP