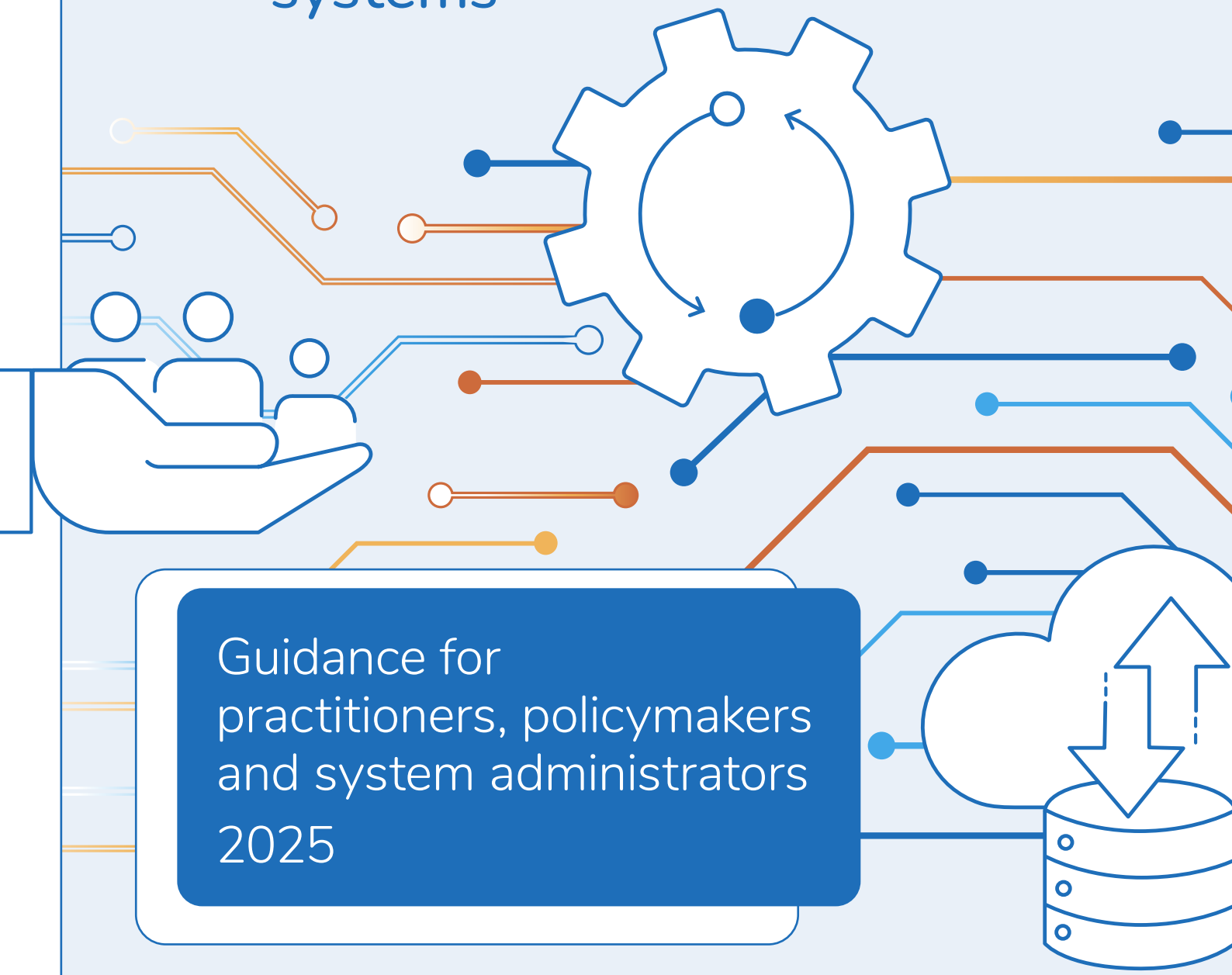
Digital Convergence
USP2030

A data governance framework for digital social protection systems



Guidance for practitioners, policymakers and system administrators

2025

Digital Convergence Initiative (DCI)

DCI is the global initiative for the digital transformation of social protection systems. Established as part of the USP2030 partnership, the DCI is an open and collaborative platform for governments, development partners, civil society organizations and the private sector united by a shared vision: expanding the coverage of social protection and enhancing its delivery through inclusive, interoperable digital systems.

Visit our website at ▶ spdci.org

Publication Survey

Your opinion is valuable to us.

Please ▶ click here to provide feedback on this publication.

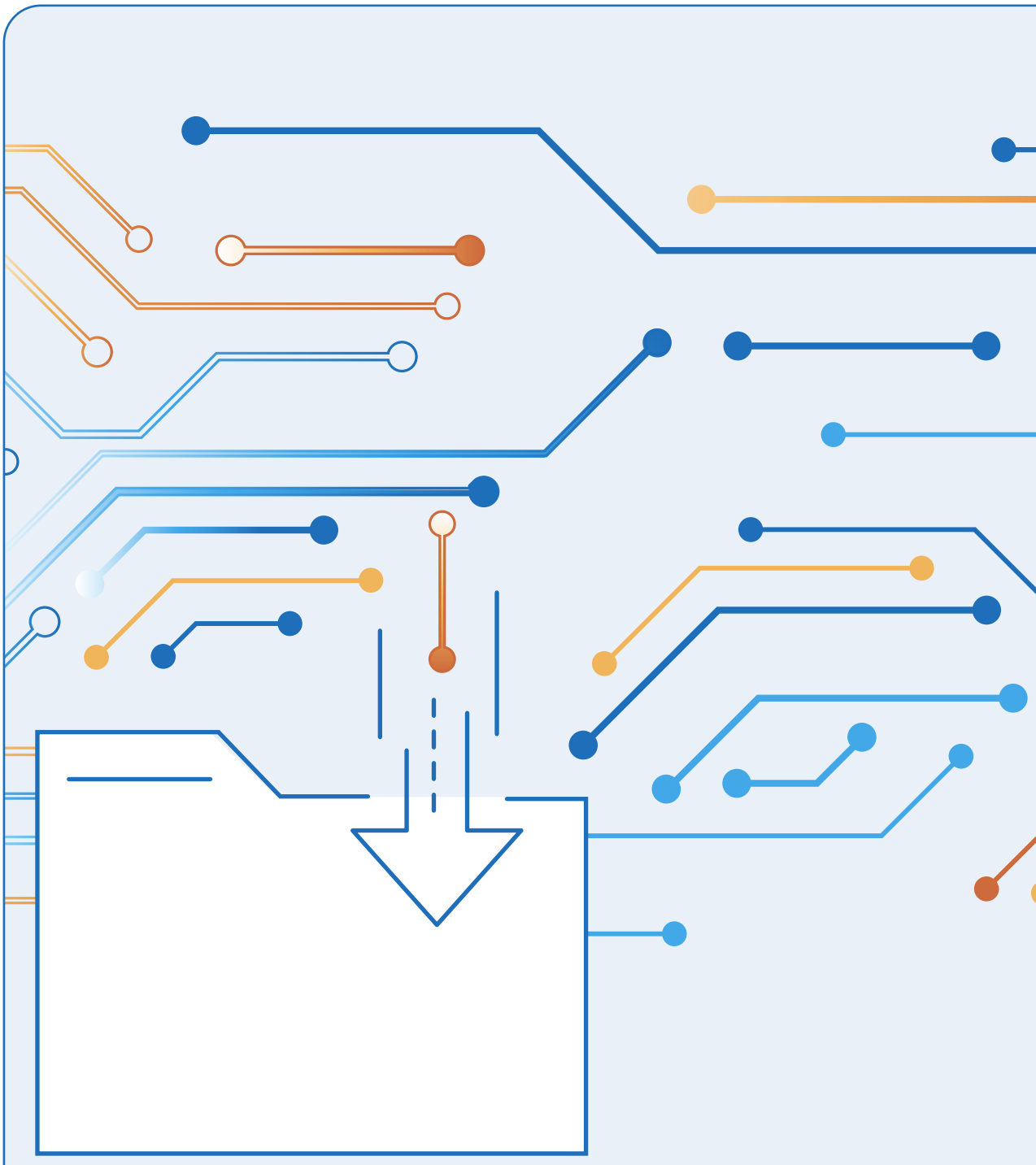
Acknowledgements

This publication builds on significant contributions from many colleagues. It was prepared by Tim Ohlenburg (Oxford Policy Management) under the guidance of Anita Mittal and Anna Deniz (GIZ, DCI). It draws on a country-specific framework developed jointly with Claude Migisha (independent consultant), which provided the foundation for the analysis. The document also reflects valuable feedback from expert reviewers, including Robert Worthington and Valentina Barca (independent consultants); Sarang Chaudhary (GIZ, DCI); Melis Guven and Mohamed Almenfi (World Bank, DCI). The country case studies were enriched by insights from Emmanuel Yeka (MGLSD, Uganda), Ercan Dansuk (MFSS, Türkiye), Johannes Paulus Acuna (DSWD, Philippines), and Veronica Acha Alvarez (MSDF, Chile).

Table of contents

List of acronyms

CAPI	Computer-Assisted Personal Interviewing
CRVS	Civil registration and vital statistics
DAMA	Data Management International
DMBOK	Data Management Body of Knowledge
DPIA	Data protection impact assessment
DSWD	Department of Social Welfare and Development
EDPB	European Data Protection Board
EU	European Union
GC	Data governance council
GDPR	General Data Protection Regulation
GNI	Gross national income
HR	Human resource
ICO	Information Commissioner's Office
IEC	International Electrotechnical Commission
ISAS	Integrated Social Assistance System
ISO	International Organization for Standardization
IT	Information technology
MIS	Management information system
NIST	National Institute of Standards and Technology
NUSAF	Northern Uganda Social Action Fund
ODI	Open Data Institute
OMB	Office of Management and Budget
ONS	Office of National Statistics
PMI	Project Management Institute
PMT	Proxy means test
RACI	Responsible, accountable, consulted, informed
UID	Unique identifier
UK	United Kingdom
UNECE	United Nations Economic Commission for Europe
UNICEF	United Nations Children's Fund
US	United States
USSD	Unstructured Supplementary Service Data



Introduction

Introduction

The need for a data governance framework

The **rapid digitalisation of social protection systems** is transforming how governments collect, manage, and use data to deliver essential social assistance and insurance programmes. Driven by advances in technology and connectivity and intensified by the COVID-19 pandemic (ODI, 2023), digital platforms that leverage administrative data are becoming central to expanding the coverage, accuracy, and responsiveness of social protection schemes (Barca et al., 2023a). The promise of artificial intelligence enhancing efficiency and responsiveness provides further momentum to evolving practices. This pivotal shift is not merely a technological upgrade, but a wide-reaching transformation that can make social protection systems more agile, inclusive, and impactful. At the same time, it introduces significant challenges for the effectiveness and responsible handling of public administration.

Data governance is at the heart of harnessing digital systems for social benefit. However, getting it right is critical to its impact on the effectiveness, inclusivity, and legitimacy of social protection systems. Sound governance ensures that data is accurate, secure, and used ethically. The resulting trust among beneficiaries, policy makers, and the general public is a core component of achieving desired outcomes, as UNICEF (2021) points to in the context of children's data. Moreover, well-governed and, thus, well-managed data facilitates timely and accurate decision making to help funnel resources to those who need them most.

Conversely, poor data governance can have serious consequences. For example, data breaches, including breaches related to personal data, such as unauthorised access, use, or disclosure, and manipulation erode trust and hinder the cooperation and support that social protection systems depend on. Inaccurate or outdated information will impair service delivery and undermine outcomes for vulnerable populations. System disruption from technical failure or attacks can harm operations, and manipulation can result in corruption or fraud. Significant investments in cybersecurity, digital infrastructure, human resources and staff training, suitable institutional arrangements and adequate fiscal space are necessary to eliminate, reduce, mitigate and manage such risks. The potential loss of citizens' trust in government is another important risk that appropriate practice can mitigate.

At present, **no data governance framework tailored to social protection exists** that countries can use to guide the development of their sector. This publication aims to fill the gap between general guidance, such as the Broadband Commission's Data Governance Toolkit (Broadband Commission, 2025), and the specific requirements of the social protection sector. Based on a review of the extensive and growing literature on the topic, we have selected recognised resources for adoption and adaptation. At the highest level, the proposed Framework begins with four broad themes that the Open Data Institute identifies as the '**four foundational pillars**' of data governance (ODI, 2023): management, quality, access, and security. These provide a broad framing that serves to focus attention and resources on key components.

Each pillar is clearly defined through **established standards and recognised organisational approaches**. The Management Pillar uses the concept of the science data lifecycle from Shah (2021), which provides a comprehensive view of the stages of data handling. The Quality Pillar relies on the dimensions of data quality outlined in Data Management (DAMA) International's Guide to the Data Management Body of Knowledge (DAMA, 2017), interpreted specifically for digital social protection systems. The Access Pillar draws on the principles of the United Kingdom's Data Sharing Governance Framework (Government Digital Service, 2022). The Security Pillar draws on the International Organization for Standardization's (ISO's) 27000 family of information technology security standards (ISO & IEC, 2022) to highlight the core components required for the confidentiality, integrity, and availability of social protection data. Finally, a process for adjusting the Framework to the particular needs of a national context takes inspiration from the US National Institute of Science and Technology's Cybersecurity Framework 2.0 (NIST, 2024). The European Union Agency for Cybersecurity (ENISA[1]) also provides useful guidance on a number of topics addressed here.

Regarding **applicability**, the composite nature of this Framework reflects the diverse components of data governance and the manifold organisational structures of social protection around the globe. The guidance on these pages is intended to provide a foundation and starting point for policy development. It should not be interpreted as a static, technical manual, as its content will need to evolve with policy and technology. Nor is it intended as a compliance standard, given the essential need for alignment with national laws and regulatory contexts. While the Framework aims for breadth and comprehensiveness in addressing core data governance aspects, it cannot fully capture the complexities faced by each country. Irrespective of these constraints, we hope that the Framework will provide impetus and a clear direction on the sector-wide, careful, and continuous effort required for modern data governance in support of timeless social protection principles.

1 See ▸ **https://www.enisa.europa.eu/topics/digital-identity-and-data-protection** for guidance on data protection and digital identity.

Objective and target readership

The ultimate rationale for all aspects of good data governance is the **provision of more efficient, effective, fair and convenient social protection to those in need**, i.e., social protection applicants and beneficiaries; hence, this is the objective of this Framework.

The readership envisaged for this Framework consists of two groups: the global social protection practitioner community and the governments of countries looking to enhance governance:

- **Social protection practitioners**: This first comprehensive mapping of data governance in the social protection space offers an opportunity to consider the relevance of this field. It may also facilitate a dialogue on the suitability of the proposed solutions. An emerging consensus can inform future iterations of this work to create a resource that promotes the evolution of standards over time. The objective is to shape the sectoral discourse towards a structured approach to the topic that ultimately leads to better policies for applicants and beneficiaries of social protection systems.
- **Policy makers and social protection system administrators**: A detailed template that maps from broad principles to specific tasks can provide a useful basis for sectoral reform and the establishment of an effective data governance framework in support of national policy objectives. This document aims to provide such a template.

Guiding lights for this document include the Digital Development Principles (Digital Principles Working Group, 2024) and widely accepted data protection principles, such as those embodied in the European Union (EU) General Data Protection Regulation (GDPR) (European Union, 2016).

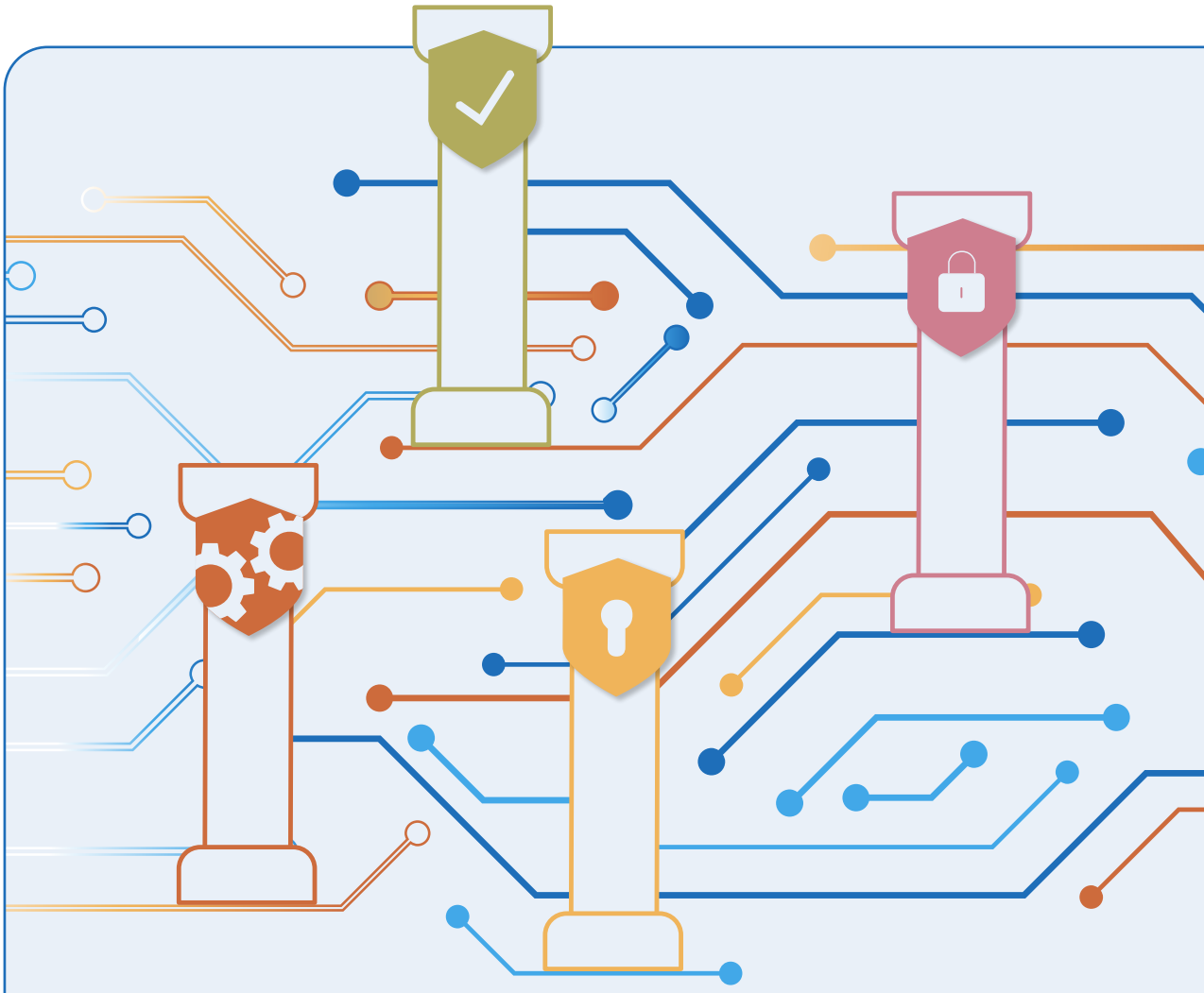
Limitations

A few words of caution are in order in relation to this Framework. It is general in nature and builds on external standards and examples, thus absorbing their flaws. It is not a legal or compliance instrument and sidesteps country-specific constraints such as statutory data-sharing prohibitions, sectoral privacy rules, and procurement restrictions. The proposed roles, RACI (responsible, accountable, consulted, informed) assignments, and implementation mechanisms are illustrative templates that require local adaptation. In settings with limited connectivity, fragmented registries, or scarce human capacity, some mechanisms may be infeasible or burdensome. Trade-offs are also context-dependent, and the balance between topics – such as interoperability versus data minimisation, or openness versus confidentiality – needs to be assessed afresh in each case.

In addition, the document's scope is shaped by its origins in country cases and a literature base that cannot reflect the full diversity of social protection architectures, including aspects such as adaptive response and humanitarian support. The small selection of case studies is illustrative rather than evaluative. They should not be read as endorsements of particular technologies or policy approaches, nor as evidence of their general effectiveness. As data governance practices, standards, and technologies evolve rapidly – especially around AI, security, and regulatory standards – the Framework needs to become a 'living document' that benefits from stakeholder feedback, periodic review, and iteration.

Outline

This report is presented in **four main parts**. Part 1 provides an *overview* of the entire document, introducing its concepts and the Framework architecture. It discusses the levels of analysis, which go from broad pillars down to implementation mechanisms, and previews the pillars as the main components of the Framework. A summary table provides an overview of the entire Framework and concludes the introductory material. Part 2 goes into detail about the *four pillars* of data governance, namely: management, quality, access, and security. Each section breaks down a pillar into its key building blocks and suggests implementation mechanisms for each. In view of the wide-ranging nature and extensive administrative requirements of data protection, Part 3 provides implementation guidance, outlining strategies for customising the Framework for staged *implementation* over the medium term. This is followed by Part 4, which sets out the country case studies. Finally, the concluding remarks reiterate key insights and round off the Framework narrative.



Part 1. Framework overview

Part 1. Framework overview

This overview section introduces the multi-tier structure of the proposed Data Governance Framework. A discussion of the pillars of data governance, down to the roles and responsibilities of the different actors in the process, completes the conceptual part of the overview. A summary table synthesises the content of this section in a compact format.

Framework structure and levels

This report proposes a Framework with five levels of detail (as illustrated in Figure 1):

- **Level 1**: The *first level* is what we refer to as the **pillars** of data governance, or the major subject areas, which jointly ensure a comprehensive account of the field. These are management, quality, access, and security.
- **Level 2**: In the *second level*, each of the abstract pillars have several '**building blocks**' that break the pillars down to more concrete areas. For instance, data quality can be decomposed into: completeness, accuracy, timeliness, consistency, and validity.
- **Level 3**: The **third level** of the Framework proposes concrete tools for operationalising the building blocks through **implementation mechanisms**. For instance, timeliness can be operationalised through appropriate data acquisition policies, data sharing agreements, and service level agreements.
- **Level 4**: The *fourth level* assigns specific tasks to particular actors (i.e., **roles and responsibilities**) in a typical social protection sector. As an example, the formulation of an acquisition policy for household interviews could be coordinated by the social registry as the actor responsible for designing the policy and drafting a policy paper, with the data governance council bearing ultimate accountability for the policy. The data collector would be consulted regarding the practical aspects of data collection in the local context, institutions that administer programmes would be consulted on their data needs, and other public data providers as well as public IT services would be consulted on a mechanism for discrepancy resolution in cases where household interviews reveal differences to existing records.

- Level 5: The *final fifth* level outlines key tasks involved in putting the implementation mechanisms into practice and assigns these to the various actors to provide a practical view of which actions need to be undertaken by which parties. These tasks are illustrative and need to be tailored to the specific implementation setting.

▶ Figure 1 showcases the different levels by zooming into a particular example.
▶ Table 1 gives an overview of the full Framework.

The four pillars of data governance and their building blocks

The proposed Data Governance Framework is organised around what the Open Data Institute (ODI, 2023) refers to as the four foundational pillars of data governance.[2] These pillars are complementary and interwoven, and critical to ensuring that data in the social protection sector is accessible, accurate, complete, and secure to enable robust and effective programme operations. Each of the pillars consists of 'building blocks' that jointly make up the pillar's broad concept. The pillars are described briefly here (see ▶ Part 2 for a full discussion).

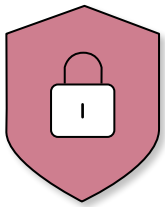
- Pillar 1. Management: Data management focuses on policies and procedures for efficiently and effectively collecting, processing, storing, and deleting data throughout its lifecycle. For this pillar, the building blocks consist of six critical stages of the data lifecycle (as formulated by Shah et al., 2021). They are: (i) planning, (ii) acquisition, (iii) processing, (iv) analysis, (v) sharing and usage, and (vi) archiving/erasure. Data management is critical and, if well done, supports reliable operations and brings about operational efficiency and regulatory compliance. It helps remove erratic policy implementation and non-compliance, which can trigger reputational risks.

- Pillar 2. Quality: Data quality deals with procedures and processes that ensure data is accurate, consistent, complete, and reliable. The building blocks of data quality are the DAMA-DMBOK2 (DAMA, 2017) set of six dimensions, namely: (i) completeness, (ii) accuracy, (iii) currency, (iv) consistency, (v) validity, and (vi) uniqueness. Data quality aspects may include accurate enumeration, data rectification, data quality assurance and control, and complete household listing. In the context of social protection, data quality enables better eligibility determination, operational efficiency, and compliance, ultimately improving public satisfaction. Poor-quality data can lead

2 The four data governance pillars proposed by ODI are neither the only nor necessarily the most correct approach to structuring data governance. However, in the absence of a canonical alternative that applies in this context, it was selected to provide a simple and intuitive frame that provides structure without overwhelming non-technical audiences with unfamiliar concepts. In contrast, the DAMA Wheel of the DAMA-DMBOK2 (DAMA, 2017) has 10 components, some of which go beyond the scope of the present publication.

to mistakes in beneficiary selection, attribution of the wrong benefit package, and dissatisfaction with public services. Principles of good administration – including the right to be heard, a fair procedure, and duty of care – should not be undermined (see Enqvist, 2023 for a case study from Sweden).

- Pillar 3. Access: Data access focuses on policies and mechanisms that ensure authorised users can efficiently retrieve and use data while maintaining data security, personal data protection and privacy,[3] and compliance. The pillar categorises the different users or consumers of the data according to their respective access levels. Accordingly, we formulate its building blocks as: (i) internal users, (ii) external users, (iii) the general public, and (iv) general considerations that cut across all. As social protection databases hold sensitive personal data, key considerations, such as referring to existing legislation around data privacy, first classifying the data according to sensitivity level, or conducting a data protection impact assessment before opening some of the data, are explored under this pillar. Data access management also helps to contain possible data breaches, foster transparency, and empower staff and institutions to leverage data effectively.



- Pillar 4. Security: Data security covers the measures and protocols implemented to protect data from unauthorised disclosure, as well as access to data, accidental or unlawful destruction, loss, alteration, and other threats. Any technical processes employed to collect, process, store, use or share data should employ robust security mechanisms, for which threshold guidelines need to be defined. Data security has four building blocks, all referred to as 'measures', in accordance with ISO 27000 (ISO & IEC, 2022), which are based on: (i) technical measures, (ii) organisational measures, (iii) physical measures, and (iv) people measures. In many settings, public sector entities must comply with personal data protection and security standards, but further security and safety measures can be built and ensure that data security is instituted right from the design of technologies and processes, which fosters trust.

Each of these four pillars is explored in ▶ Part 2 of this document. Further explanation of the building blocks, as well as more detailed information on levels 3, 4 and 5 of the Framework, is provided in the respective sections. Before turning to such in-depth discussion, it is worth understanding the overarching roles and responsibilities vis-a-vis data governance (Level 4), as these cut across the different Framework pillars.

3 The term data protection focuses more on the technical and organisational measures needed to secure personal data, privacy focuses on empowering individuals with control over their personal information and ensuring transparency and respect for individual rights. This publication refers to both simply as 'data protection'.

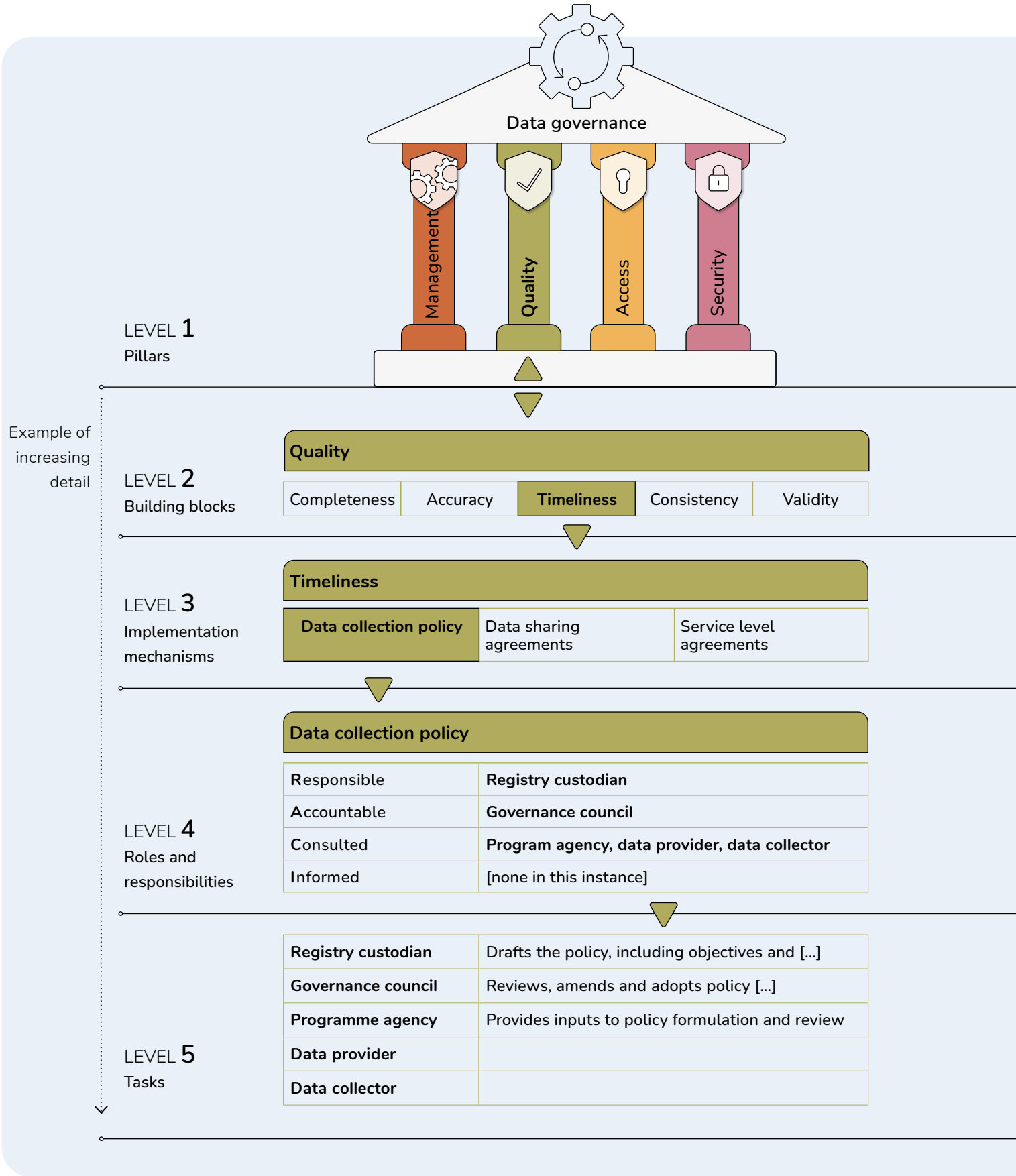


Figure 1. Structural levels of the Data Governance Framework
Sources: Pillars based on ODI (2023), quality building blocks based on DAMA (2017)

Roles and responsibilities

The architecture of social protection information systems varies widely, reflecting the diversity of programmes and institutions that make up the sector in different countries. Programme management information systems, social registries, and beneficiary registries are common data infrastructure designs, and it is not possible here to provide detailed recommendations for each type. Nevertheless, the core data exchange relationships are similar across national set-ups, and we can refer to key roles that are found in most. In practice, a single institution may fulfil several of these roles, or they may be split. But data governance requirements are linked to the functions and tasks inherent in data exchange, regardless of particular institutional boundaries; the following material should be interpreted accordingly and adapted to the specific architecture found in a given policy setting. A stylised view of these roles and associated data flows is provided in Figure 2, followed by a brief description of each type of actor.

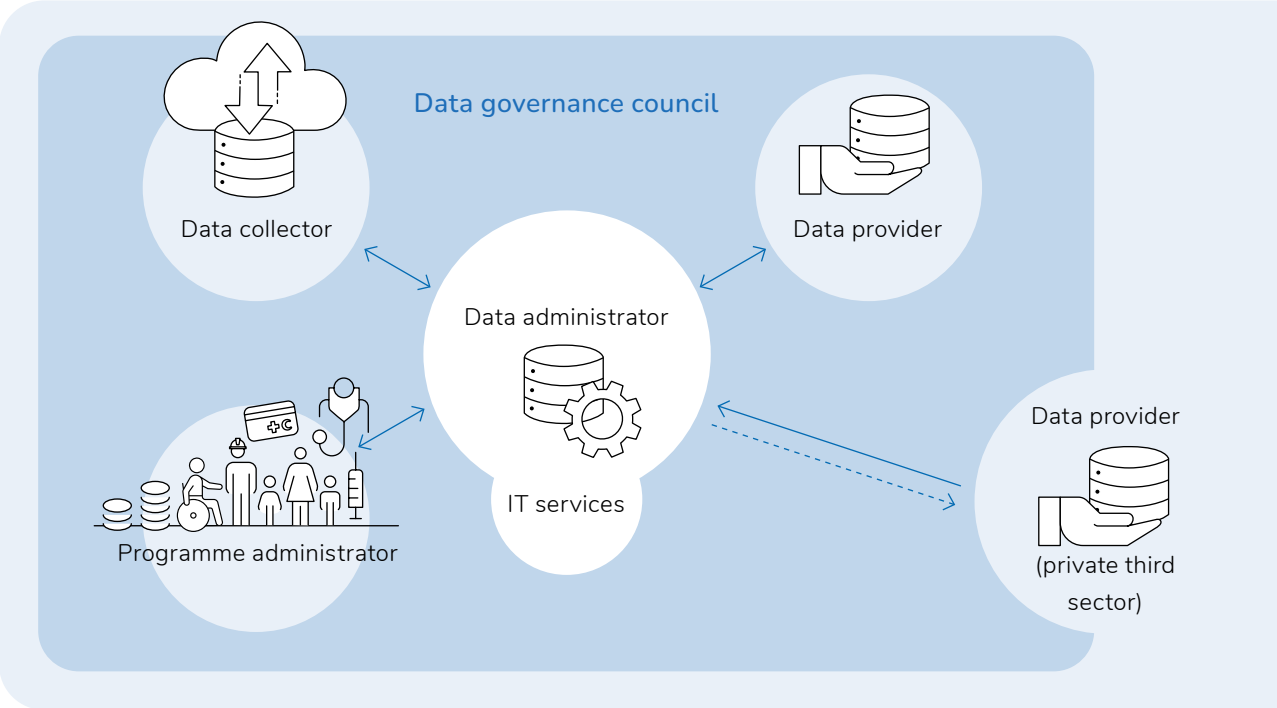


Figure 2. Stylised overview of data governance roles

- Data governance council: Data governance is a sector-wide endeavour that is best overseen by a body that takes the same perspective. As various institutions may contribute to sector data and interact with the relevant database, a governance council comprised of senior representatives from the main stakeholders would provide suitable oversight. The role of the council is to oversee the sector's operational performance, to propose, evaluate and sign off on policy, and to coordinate the activities of sector members. In its role bearing ultimate responsibility for the

sector's data governance, it has the power to convene and the ability to determine solutions on contentious topics. Senior council members would likely delegate representation to a mid-level staff member and reserve participation to occasional high-level meetings, at which periodic review and major policy directions would be discussed. A secretariat may be constituted to carry out its functions.

- **Data administrator**: Data for social protection operations may be stored in one or several programme management information systems (MISs), in a social registry, or a beneficiary registry – in this document, we generally refer to these as a social protection database. The assumption in this text is that this information is curated by a policy maker who assumes a policy design, coordination, and digital service execution role. Technical database administration tasks also fall under this role, but a wider remit is intended in this description. In practice, some of the tasks involved in this role might be split with the IT services role (discussed below), with the distinction between the two lying in the focus of IT services on purely technical matters. The office of the organisational unit that administers the social protection data would often be a suitable host for the data governance secretariat that a data governance council may wish to create.

- **Programme administrator**: A given social protection programme may be provided by one of a variety of possible institutions. This text refers to such providers as programme administrators and assumes an operational and policy-implementation role for them. The institution may manage their data and IT systems, in which case they would also play the role of data administrator and of IT services, or even data collector.

- **Data collector**: The collection of primary data during personal or household interviews remains an important data acquisition method in many social protection systems. The results of such a registration exercise may account for a large part of the information that the sector holds. The data collector may be constituted by several entities, such as when multiple survey firms are contracted to cover different parts of the country. It could also be that a programme administrator wishes to commit the resources needed to conduct primary data collection. The assignment of the national statistics agency to collect this data is also common.

- **Data provider**: Data providers create relevant information as part of their regular operations, such as demographic data being produced by civil registration, or some types of asset ownership being evident due to land and vehicle registries. Most data providers are likely to be public sector bodies, but they may also include private and third sector entities. From the perspective of this text, data providers are generally assumed to be separate institutions from the data and programme administrators.

- **IT services**: IT services are conceived of here as a public agency that provides government entities with infrastructure and services as well as software support. The IT role envisaged for the social protection sector is to operate the social protection database's technical infrastructure, including data portals, as well as providing IT services to other actors in the sector, as required. IT services do not collect or share data directly, but provide the means for others to do so securely and efficiently. In some settings, IT services are housed within each institution, in others they provide

services for the sub-bodies of a large central entity, and in yet others central IT services exist, but their tasks are the same regardless of their parent institution.

- **Across all stakeholders – RACI responsibility assignment**: Each implementation mechanism (Level 3 of the Framework) is handled by a certain set of actors. The discussion of each pillar, therefore, includes a table that lists a key set of responsibilities for the various roles. We have applied a Responsibility Assignment Matrix (PMI, 2021) to describe the involvement of various roles vis-a-vis the implementation tasks or deliverables. Attractive due to its relative simplicity, the purpose of this matrix is to clarify responsibilities. The matrix has four parts, with one for each letter:

  - Responsible generally refers to the actor tasked with carrying out a task or achieving its completion.
  - Accountable signals the actor who carries the ultimate administrative or political responsibility for a task.
  - Consulted refers to actors whose responses feed into the implementation process.
  - Informed means the actor who receives information regarding the mechanism's execution or completion.

  Taken together, this description provides an easily accessible summary of responsibilities by role.

As with any other aspect of the Framework, it is worth noting that this approach can be adapted or changed as desired. ▶ Part 3 on implementation provides additional guidance in this regard.

Framework summary

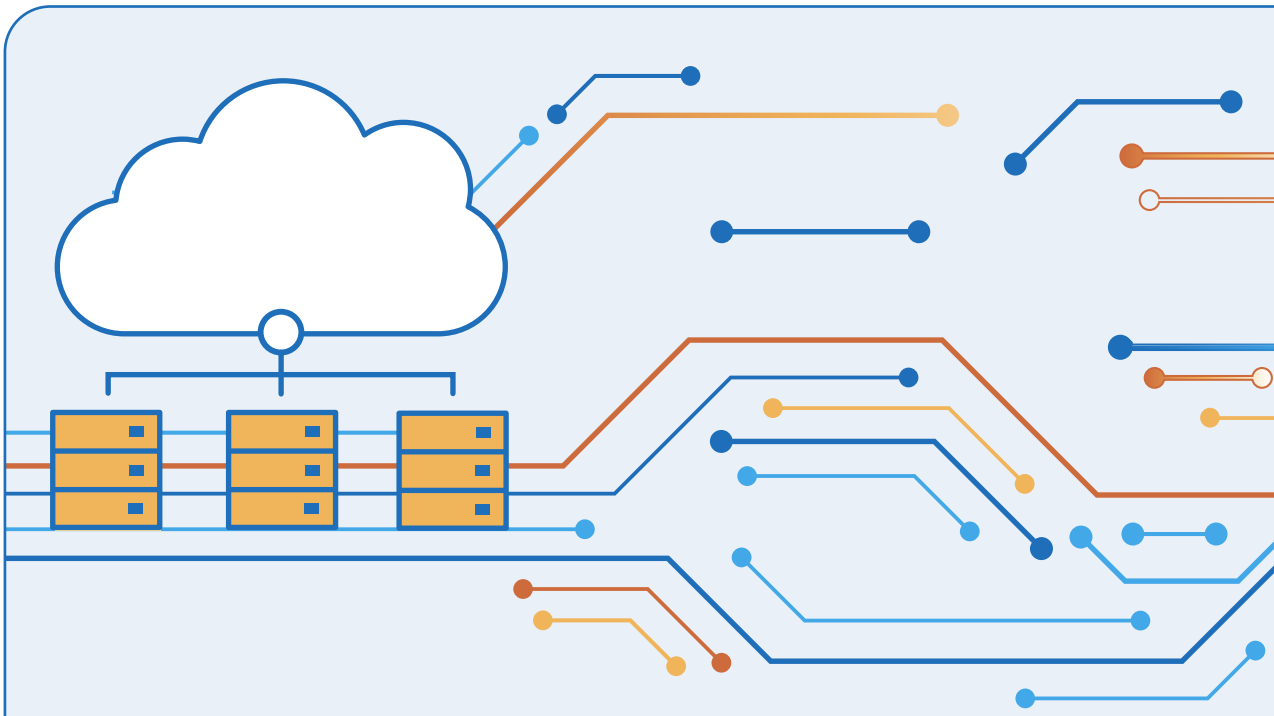
Table 1 provides a summary of the Data Governance Framework, which serves as a reference and a general overview. Each of the four pillars is split into its core building blocks, which function as thematic groups. Within these blocks, particular implementation mechanisms are proposed that operationalise it, in part or in full. A proposed priority level indicates the potential importance hierarchy of adapting the various mechanisms. Further pillar-specific tables in Part 2 outline roles and responsibilities in further detail (see tables ▶ 2, ▶ 3, ▶ 4 and ▶ 5).

Table 1. Summary of Data Governance Framework

LEVEL 1: Pillar	LEVEL 2: Building block	LEVEL 3: Implementation mechanism	LEVEL 4: Roles and responsibilities	Priority
Management	Planning	Data management plan	R: DA; A: GC; C: DP, DC, PA, IT	Intermediate
	Acquisition	Data acquisition policy	R: DA; A: GC; C: PA, DP, DC	Immediate
		Registration form design	R: DA; A: GC; C: DC, PA, I: IT	Immediate
		Data sharing agreements	R: DA, DP; A: GC; C: IT	Immediate
		Service level agreements	R: DA, DP; A: GC; C: IT	Immediate
	Processing	Eligibility process documentation	R: DA; A: GC; C: DP, DC, PA, IT	Intermediate
		Eligibility determination	R: DA; A: GC; C: IT, DC, DP; I: PA	Immediate
		Exit process	R: DA; A: GC; I: PA	Intermediate
	Analysis	Data catalogue	R: DA; A: GC; C: IT, DP, DC, PA	Immediate
		Data protection impact assessment	R: DA; A: GC; C: PA, IT, DC, DP	Immediate
		Logs, dashboards and monitoring	R: IT; A: DA; C: DC, DP, PA; I: GC, PA	Intermediate
	Use, sharing and publication		[see Access Pillar]	
	Archiving and deletion	Data retention policy	R: DA, IT; A: GC; C: PA	Intermediate
		Data archive	R: IT; A: GC	Intermediate
Quality	Complete-ness	Validation and reconciliation	R, A: DA; C: DC, DP; I: GC	Intermediate
		Self-declaration	R: IT, DA; A: PA	Intermediate
	Accuracy	Registration officer training	R, A: DC; C: DA, PA	Immediate
		Pilot registration	R, A: DC	Intermediate
		Real-time monitoring	R, A: DC; I: GC, DA	Intermediate
		Access and rectification modality	R: DA, IT; A: DA; I: PA, GC	Intermediate
	Currency	Data acquisition policy	R: DA; A: GC; C: PA, DP, DC	Immediate
		Data sharing agreement	R: DA, DP; A: GC; C: IT	Immediate
		Service level agreement	R: DA, DP; A: GC; C: IT	Immediate
	Consistency	Pre-populated Computer-Assisted Personal Interviewing (CAPI)	R: IT, DC; A: DC; C: DA; I: DA	Intermediate
		Discrepancy resolution process	R: DA, DP, DC; A: GC	Intermediate
	Validity	Data catalogue	R: DA; A: GC; C: IT, DP, DC, PA	Immediate
		Data sharing agreement	R: DA, DP; A: GC; C: IT	Immediate
	Uniqueness	Master data model	R: DA, IT; A: GC; C: DP, PA, DC	Immediate
		Unique identifier	R: IT; A: GC; C: PA, DA	Immediate

Access	Internal access	HR database	R: DA; A: GC; C: PA, DC, DP, IT	Intermediate
		Account permission and revocation	R: IT; A: GC	Immediate
	External access	Data sharing agreement	R: DA, DP; A: GC; C: IT	Immediate
		Discrepancy resolution process	R: DA, DP, DC; A: GC	Intermediate
		Secure sharing modality	R: IT; A: GC	Immediate
	Open data	Anonymisation process	R: DA, IT; A: GC; C: PA, DC, DP	Intermediate
		Release approval process	R: IT; A: GC	Intermediate
		Data portal	R: IT; A: DA; I: GC	Intermediate
	Cross-cutting issues	Data access policy	R: DA; A: GC; C: PA, IT	Intermediate
		Access request process	R: IT; A: GC; C: DP, DC, PA; I: DP, PA	Intermediate
		Consent management	R: DA, IT; A: GC; C: DC, PA; I: DP, PA	Immediate
Security	Technical	Encryption	A, R: IT; I: GC	Immediate
		Authentication	R, A: IT; I: GC	Immediate
		Data loss prevention	R, A: IT; I: GC	Immediate
		Network security	R, A: IT; I: GC	Immediate
		Endpoint security	R, A: IT; C: DA, PA, DC; I: GC	Immediate
		Patches and updates	R, A: IT	Immediate
		Penetration testing	R, A: IT; I: GC	Intermediate
	Organisa-tional	Incident response plans, disaster recovery and business continuity	R: IT, DA, PA; A: GC	Intermediate
		IT supplier risk management	R: DA, DC, DP; A: GC; C: IT	Intermediate
		Regular security review	R: IT; A: GC; C: PA, DP, DC, DA	Intermediate
	Physical	Secured access	R: DA, PA, DP, DC, IT; A: GC	Immediate
		Device protection	R: DA, PA, DP, DC, IT; A: GC	Immediate
		Backup and recovery	R, A: IT	Immediate
	People	Training	R: DA, PA, DP, DC, IT; A: GC	Intermediate
		Insider threat management	R: DA, PA, DP, DC, IT; A: GC	Intermediate

Key: Responsible (R): data administrator (DA); Accountable (A): data governance council (GC); Consulted (C): data provider (DP), data collector (DC), programme agency (PA), IT services (IT), Informed (I)



Part 2. Pillars of data governance

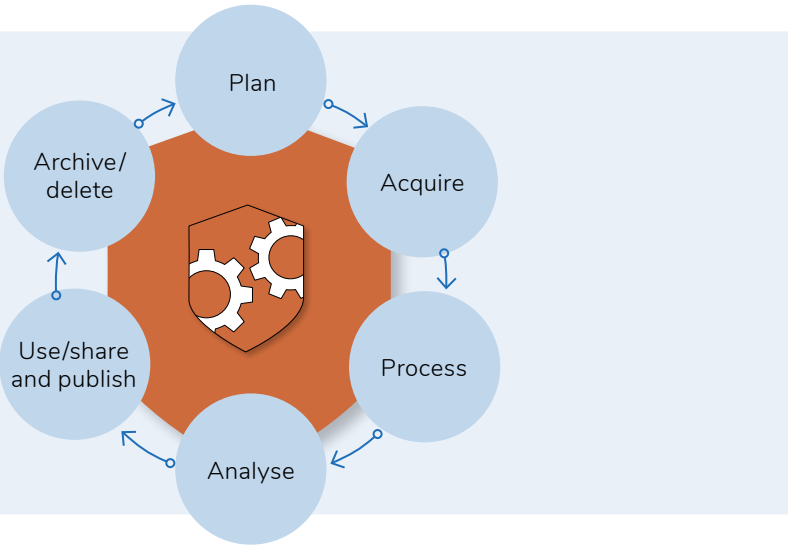
Part 2. Pillars of data governance

Pillar 1: Management

Data management is a critical pillar of the proposed Data Governance Framework. It comprises six stages across the data lifecycle (see Figure 3[4]): (i) plan, (ii) acquire, (iii) process, (iv) analyse, (v) use and share/publish, and (vi) delete/archive. The use/share and publish building block is discussed under Pillar 3: Access. The remainder of this section delves into each of the six stages in turn, which we refer to as Level 2 'building blocks' in the overarching Framing (▶ Figure 1). In each block, we discuss implementation mechanisms (Level 3) that provide practical tools. As a summary of the overall pillar and to provide additional detail, the section concludes with a RACI matrix that assigns roles and responsibilities (Level 4) in terms of specific tasks (Level 5).

Figure 3.
Data management pillar lifecycle

Source:
Shah et al. (2021)



Planning

Ambitions and plans around leveraging data to advance social protection must be captured in a data management plan (Level 3: implementation mechanism). This plan outlines the goals, how they will be achieved, and the responsibilities (institutional,

4 This lifecycle is an adaptation of the social protection setting of Shah et al.'s (2021) data lifecycle framework for data-driven governments, which is itself derived from the recognised US Geological Survey science data lifecycle model (Faundeen et al., 2013).

individual). Social protection is a multi-stakeholder domain – within and beyond government – so drafting this plan needs to involve all the stakeholders outlined in Part 2 at their respective levels of involvement. The data management plan offers information about key concepts (i.e. data lifecycle, security, sharing, etc.) and responsibilities. Ultimately, this plan needs to unlock the value of data in response to the various needs to deliver efficient and effective social protection programmes.

Data management plan

A data management plan is a document of instructions on data handling throughout the data lifecycle, including considerations of risk management and mitigation, which loom large with social protection data. It can serve as an overall policy document for the Data Governance Framework if acquisition and access policies are integrated or referenced under the relevant lifecycle steps. The plan can tie the various pillars of data governance together into a coordinated whole and provide an operational document that uses and implements the Framework, as proposed on these pages. In doing so, the plan can ensure that day-to-day data management and governance practices align with policy objectives and compliance requirements. Canonical references for data management plans include the DAMA-DMBOK2 (DAMA, 2017) and the ISO/IEC reference model of data management (ISO & IEC, 2003).

Data management plan	Instructions on data handling throughout the data lifecycle.
Components Data flow mapping	A diagram that illustrates current data flows from and to the various steering group members. A version that adds further stakeholders can serve as a planning tool for the possible expansion of scope and functionality. Such mapping is a first step in creating a master data model, discussed under the Quality Pillar.
Framework summary	An expanded Framework summary table, as in Part 1, Framework Overview, which shows the various building blocks and implementation mechanisms by pillar and assigns tasks to particular roles. The data governance council may serve as a reference document for Framework implementation.
Lifecycle toolkit	A listing of the various implementation tools along the data lifecycle that can serve as a compendium of data governance policies, processes, tools, and mechanisms.
Priority	Intermediate

Acquisition

Data collection plays an increasingly critical role in today's digitalised social protection systems; hence, its acquisition merits particular attention. Where it is conducted, primary data collection via person- or household-level data collection is a major logistics exercise that is key to data quality. Data acquisition from across the public sector is the other main form of acquisition and is at the heart of interoperability. Third party data generally play a less prominent role, but that may change as data and technology evolve and should be addressed where relevant.

Data acquisition policy

A data acquisition policy is a guideline document that provides directions and procedures for data collection. It contains specific instructions for the three acquisition building blocks – primary collection, administrative data, and third-party data – as these all require very different approaches. Data acquisition overlaps with the other aspects of data governance, particularly with issues to do with data quality such as completeness, validity and accuracy. An example of a data acquisition policy that holds useful lessons is that of the United Kingdom's (UK's) Office of National Statistics (ONS, 2023).

Data acquisition policy	Guidelines that provide directions and procedures for collecting data.
Components Scope	A statement on the intended contents of the data items in terms of the types of information to be collected (also see ▶ the sub-sections on 'Registration form design' and 'Data catalogue' in Pillar 1).
Data sources	Specific sources from which data is intended to be collected, and may already be collected, including their classification in terms of the three building blocks of primary collection, administrative data exchange, and third-party sources.
Acquisition methods	Preferred acquisition methods and specifications of their application.
Acquisition conditions	The conditions under which data is collected depend on the type of collection. For primary collection, this would include policy prescriptions regarding personal data protection requirements, the survey approach, intended frequency, and self-declaration options. For administrative data, it would include requirements formalised in the data sharing agreement. For third-party data, procurement guidelines for commercial data and other suitable arrangements for non-commercial data would be specified here.
Performance indicators	Specific, measurable, achievable, relevant, and time-bound (SMART) indicators should be set for all major policy objectives.
Repository of tools and mechanisms	Beyond objectives and general process guidance, the data acquisition policy can serve as a repository for templates and specifications for the subsequent implementation tools under this pillar. For instance, standard data sharing agreements, separate for public and non-public sectors, can be added in an appendix as a basis for institution-specific adaptation.
Review policy	The data acquisition policy itself, the tools and mechanisms it stipulates, and the data acquisition outcomes they lead to should be reviewed at set intervals, and compared with the performance indicators. Any parts that perform below potential should be updated to improve future outcomes and new performance indicators set.
Priority	Immediate

Registration form design

A registration form is a guideline document that provides the specifications for questionnaire design. In settings where data is collected from individuals or households, its purpose is to ensure that the survey instrument, which is an essential operational aspect of primary data collection, is compliant with personal data protection,[5] effective and efficient. For digital forms, the US OMB (2023) offers useful insights into creating user-centric journeys. Paper-based enumeration is covered broadly in the World Bank's report *Capturing What Matters* (World Bank, 2010) on household surveys; Wagner et al. (2022) provide additional guidance on data protection.

Registration form design	A guideline document that provides the specifications for questionnaire design.
Components Collection principles	In view of the high collection cost of large social protection databases, which often cover a substantial part of the population, a minimal questionnaire is advisable and, indeed, required by the personal data protection principle of data minimisation. Socio-economic sample surveys can be used to establish relevant statistics such as programme uptake, whereas the intake and registration instrument should be limited to necessary items of administrative utility (e.g. currently used by current or potential user programmes for their targeting, or necessary to support programme operations). Variables should also be prioritised for high time-validity (e.g. no food consumption over last seven days), relatively high stability over time (e.g. no drastic fluctuations depending on seasonality) and low risk of creating perverse incentives (e.g. pulling children out of school).
Required information	Certain information items are indispensable for programme and beneficiary management. A list of these needs to be collated for the various programmes and consolidated into a list.
Variable selection principles	Where proxy means tests (PMTs) or similar scoring approaches are used for the assessment of needs and conditions, the information needed can be informed by variable selection methods. Exclusion criteria, for instance, due to sensitivity (e.g. religion) or inappropriate incentives (e.g. school attendance), should be considered for data items, to avoid unintended behavioural responses or the perception of discrimination.
Modular approach	Instead of collecting all potentially relevant data, data minimisation suggests that only relevant information should be collected. That information will vary according to the applicant profile, so that data required for particular programmes will not be needed, depending on demographic and other characteristics. For example, labour market information may not be needed for pensioner households. Organising collection by module can facilitate data minimisation.

5 As an example, for the EU, the relevant legal framework is the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, i.e. the GDPR.

Registration form design

Consent	Depending on the legal framework of a given policy context, consent for data collection and processing may need to be requested from those registering for a programme. The consent needs to be specific (relate to a clearly stated purpose), informed (giving people understandable and complete information), and limited to what is needed. A consent management system, discussed under the Access Pillar, can build on this initial consent to keep it current and allow for its revocation.
Priority	Immediate

Data sharing agreement

Data sharing agreements outline the terms and conditions under which data can be shared between parties, including the purpose of the data sharing, the types of data involved, and the responsibilities of each party. It ensures compliance with legal, organisational and security standards to protect the data and the personal data protection and privacy of individuals whose data is being shared. Examples of items to include can be found in the UK Information Commissioner's Office's (ICO's) practical advice on data sharing in its code of practice (ICO, 2021a), as well as in documents by the European Data Protection Supervisor[6] and the European Data Protection Board (EDPB).[7]

Data sharing agreement	An agreement that outlines the terms and conditions under which data can be shared.
Components Purpose	The reason for which the data is shared, which acts as a constraint on subsequent clauses.
Institutions	The identity of the institutions making the agreement.
Legal context	The applicable laws and regulations that govern the agreement.
Responsibilities	• *Permitted use*: Restriction of use to the listed purposes. • *Access policy:* Users who may have access to the data. • *Retention and disposal:* The duration for which the data can be stored and processed, and when and under which conditions it needs to be disposed of. • *Access and usage monitoring:* Procedures for monitoring access and usage, based on access logs, including a regular process for sharing the information with the data provider.
Agreement duration and termination	The time for which the agreement is valid, and under which conditions and through what process it can be terminated.
Discrepancy resolution	A process for resolving discrepancies that the data recipient becomes aware of, potentially resulting in an update of the master record (also see ▶ sub-sections on 'Discrepancy resolution process' and ▶ 'Master data model' in Pillar 2).

6 See: ▸ https://www.edps.europa.eu/data-protection/data-protection_en

7 See: ▸ https://www.edpb.europa.eu/news/news/2024/edpb-clarifies-rules-data-sharing-third-country-authorities-and-approves-eu-data_en

Data sharing agreement	Legal requirements	• *Liability:* Details on the liability that each party assumes. • *Completion requirements:* Conditions for the agreement to enter into force, including data security, personal data protection, and other relevant legal requirements. • *General clauses:* Additional provisions, as relevant and required.
	Variable listing	The data to be shared, potentially including the relevant information from the provider's data catalogue, including formats, encoding, and other meta-data. Should be limited to the minimum set of variables needed for the agreed-upon purpose.
	Data transmission method	The manner in which the data will be shared securely.
	Exchange frequency	The frequency at which the provider will send, or the recipient will collect updated information.
	Security measures	Additional security measures to be taken beyond the recipient's standard operating procedures.
	Financial settlement	Any financial implications of the agreement, including penalties for mishandling and misuse.
	Authentication	Alignment with the organisation's data access policy and permissioned user accounts.
	Technical specifications	Details of the data exchange modality, including technical aspects such as API request specifications, can be added in an appendix to the agreement as a coordination mechanism.
	Two-way exchange safeguards	In cases where data is provided to other parties, the legal basis for data sharing needs to be clarified and consent sought where necessary (see ▶ sub-section on 'Consent management' in Pillar 3). A data protection impact assessment should also be prepared to consider the possible risks involved and decide accordingly whether sharing is warranted (see ▶ sub-section on 'Data protection impact assessment' in Pillar 1).
Priority		Immediate

Data sharing agreement (non-commercial data)

A data sharing agreement with institutions that provide data to the social protection database on non-commercial terms can be handled with a data sharing agreement similar to that described in the previous point. Legal counsel should be consulted in each case to ensure that the agreement is appropriate for the particular case. See ▶ sub-section on 'Data sharing agreements' (directly above) for components and priority, and adjust as required for a suitable agreement depending on the nature of the institution.

Service level agreement (commercial data)

In this context, a service level agreement is a contractual document that specifies the terms on which a commercial provider will provide data or data-related services to one of the public bodies that are stakeholders of the social protection database. It outlines the services provided (including data provision), the expected standards of these ser-

vices, and the responsibilities of both parties to the agreement. Clear specifications help to coordinate expectations, provide assurance of standards, establish accountability mechanisms, and facilitate conflict resolution if a dispute arises. The agreement may also provide for two-way data exchange, potentially giving the private sector party access to social protection data. Such arrangements are rare, and require a specific data protection impact assessment (DPIA), stringent safeguards, as well as appropriate consent (see the implementation mechanism discussed below in this pillar). An example of public sector advice on such agreements is from the US Department of Energy (2024), which particularly highlights challenges with regards to technology vendors that are highly relevant in social protection.

Service level agreement (commercial data)	A contractual document that specifies the terms on which a commercial provider will provide data or data-related services.
Components Scope of services	The data to be provided, including the data sharing modality.
Performance standards	Measures of data quality, such as completeness, timeliness, accuracy, consistency, and validity.
Availability standards	Uptime guarantees for data sharing portals, such as APIs, and similar measures of availability depending on the modality.
Support	The support services to be provided, if any.
Performance monitoring	Monitoring mechanisms and reporting requirements that document service levels.
Compliance	Any legal and regulatory requirements that the data provider needs to fulfil.
Financial terms	Remuneration details including account details, payment amounts and periods, late payment penalties, and compensation for substandard service delivery.
Priority	Immediate

Processing

At this stage, data is transformed through one or several processing steps into a format that serves operational requirements. The infrastructure must be in place to permit the required data preparation and transformation for optimal data usage. The Level 3 implementation mechanisms span many of the delivery chain functions performed by social protection information systems. An exhaustive discussion of processing activities is beyond the scope of this text. Here, we focus on eligibility determination, including assessment of needs and on what to base the decision, as an example of a processing activity. For an in-depth discussion of social protection service delivery, see Lindert et al., (2020). CORE-MIS (2025) is an example of an open-source software platform that performs a number of related processing steps.

Eligibility process documentation

Supporting eligibility determination across different programmes, each with different eligibility approaches, criteria and mechanisms, is a core processing task of many social registries (Leite et al, 2017), and its performance is a key policy concern. Clear documentation on how the determination should be developed, assessed, used and updated promotes accurate and reliable assessment. Documentation of the eligibility determination process is closely related to registration design and registration officer training, but also intersects with many data governance concerns, as it may use sensitive personal data obtained from administrative and other sources for determining eligibility.

Eligibility process documentation	Documentation describing the process for determining eligibility.
Components Data preparation guidelines	Specific instructions for converting raw applicant data into the information needed to make eligibility decisions. For instance, age-based eligibility may require calculation of age from date of birth.
Eligibility metrics	Definitions of quantitative measures of eligibility determination outcomes, to be used for policy evaluation and mechanism design.
Mechanism design	Specification of the precise criteria and assessment mechanics that determine eligibility at the household or beneficiary level, with reference to evidence-based outcomes. In the case of community-based assessment, protocols and procedures for an elicitation of household welfare rankings are needed. For proxy and hybrid means tests, statistical procedures need to be defined. For geographic criteria, the administrative areas need to be defined, with reference to available data sources and sample frames, etc.
Calibrated mechanism and instructions	The calibrated mechanism and detailed implementation instructions to be used for eligibility determination, e.g. statistical model for PMTs, the process for household ranking in a community-based approach, or the chosen (set of) criteria for categorical targeting.
Review policy	Intervals and event triggers, such as the release of a new socio-economic data, that prompt a review of actual versus expected eligibility outcomes, and a possible re-calibration on the assessment mechanism (in relation to approaches for which this is relevant).
Priority	Intermediate

Eligibility determination

The overall policy design of social protection programmes determines how the assignment of eligibility should be conducted in general terms. The task of turning such principles into actionable evidence at the applicant level requires identification of the beneficiaries who are entitled to receive social protection benefits. The process also needs to ensure that the correct number of beneficiaries is selected, in line with programme objectives and possible resource constraints. Documentation of the process is closely related, as the eligibility conditions need to be adjusted according to the observed outcomes during assessment. Leite et al. (2022) discuss possible policy choices, their practical implications, and various related issues.

Eligibility determination	Operationalising policy to determine eligibility.
Components Coverage determination approaches	Approaches for setting the target number of beneficiaries, according to population characteristics, policy objectives and budget constraints, for each of the social protection programmes that use the social protection database for eligibility determination.
Eligibility thresholds	The thresholds (if any) that result from applying the coverage determination approaches, possibly broken down by low-level administrative unit.
Anticipatory assessment	In some cases, households are likely to become eligible for certain programmes, such as old-age pension entitlements or additional child support for families with a pregnant woman. Anticipatory assessment, including timely intake and registration procedures, can facilitate policy implementation and reduce waiting times for intended beneficiaries.
Programme catalogue	A listing of all programmes that use social protection database information to record or assign eligibility, and their respective coverage determination approaches, thresholds, and review periods.
Priority	Immediate

Exit process

The exit process refers to the procedures in place to manage the transition of beneficiaries out of a programme. As social protection programmes tend to run for long periods, but are often designed for limited benefit duration, the due exit of current beneficiaries is similarly important as accurate eligibility determination, to which it is closely related. See Lindert et al. (2020) for a discussion of issues around beneficiary exit.

Exit process	The procedures for managing how beneficiaries transition out of a programme.
Components Regular re-assessment of eligibility	Implementation of a dynamic social protection system requires assessment responsive to data changes. A regular interval at which continued eligibility is verified is an important manifestation of this objective, although intervals need to be commensurate with data intake practices. Relevant data updates can also prompt re-assessment, but a set date may be more convenient in administrative process terms.
Dual threshold	In poverty-targeted (particularly PMT and household means test-targeted) programmes, small changes in household characteristics may lead to a change in eligibility status for those close to the threshold. Avoidance of frequent changes for better policy predictability on the part of beneficiaries may be achieved by a slightly lower eligibility threshold for exit versus the regular one for entry, albeit at the cost of differential treatment according to prior participation history.

Exit process	Transition period	A suitable transition of several months may be appropriate to enable beneficiaries to adjust their budgets in response to the loss of programme benefits. The period should be long enough to allow for completion of a grievance redress process, including possible rectification of data, to protect beneficiaries from administrative errors.
	Anticipatory notification	As with anticipatory eligibility assessment for likely future beneficiaries, eligibility loss is foreseeable, such as when benefits are based on household composition using age-based criteria. The notification of households expected to exit can be timed to coincide with the transition period to reduce delays in policy implementation.
	Death registration	When a beneficiary dies, their direct eligibility ceases, but that of their household may continue. Where possible, registration of death should trigger an assessment of eligibility implications, including re-assessment where appropriate. Interoperability of social protection data with civil registration data can provide automatic updates, which can then lead to follow-up activity.
Priority		Intermediate

Analysis

Data analysis is achieved by documenting the underlying metadata about key data assets according to standard operating procedures. The availability of appropriate contextual metadata paves the way for data discoverability, use, and assessment of completeness by providing a comprehensive picture of available items. Wider analysis of data use through monitoring activities and the assessment of risks to the registered population are other essential components of this building block. Relevant sources for more details include the ISO/IEC 10032 Reference Model of Data Management (ISO & IEC, 2003), the ISO 9001 (ISO, 2015) standard on quality management systems, and the DAMA-DMBOK2 (DAMA, 2017).

Data catalogue

A data catalogue provides a context and a layer focusing on discovery, search, metadata management, lineage, collaboration, and governance. In practice, a data catalogue accelerates the generation of insights by ensuring that data is readily available and accessible, with sufficient context and clearly specified access permissions. A robust data catalogue comprises five essential components: metadata, data classification, data lineage, data dictionary, and data glossary. A data catalogue lists all data items that form part of the social protection database, along with their key characteristics. It serves as a comprehensive record of data assets, facilitating quality assessments, data governance processes such as reconciliation and validation under the Quality Pillar, and integration with the human resources (HR) database listed under the Access Pillar. As an example of relevant guidance, the UK government suggests using the Data Catalogue Vocabulary (DCAT) standards in the creation of a data catalogue (Government Digital Services, 2024).

Data catalogue	A centralised inventory of data assets that organises available information and provides metadata definitions, rights, and governance information.
Components Metadata	The nature of each data item, including format, structure, creation date, last update, and related attributes. Shared metadata ensures consistency and interoperability across different sources.
Data classification	Categorisation of data by type, such as asset ownership or demographic characteristics, along with its sensitivity level.
Data lineage	Documentation of the origin of each data item, detailing sources and transformations applied, enabling traceability and auditability.
Master record	In cases where data is available from multiple sources, one source is designated as authoritative, serving as the master record, against which other sources are reconciled.
Data dictionary	A detailed reference that defines each data element, specifying its name, description, data type, allowed values, format, relationships to other data elements, and validation rules. It serves as a technical reference ensuring consistency in data entry, storage, and usage.
Data glossary	A curated collection of clearly defined business terms and concepts used within the social protection database. It ensures common understanding among stakeholders by linking business terms to their corresponding data elements and metadata, facilitating communication and data governance.
Access guidelines	A clear outline of data access protocols in compliance with personal data protection rules, permissions, and details on data sharing through formal agreements and other regulated modalities.
Priority	Immediate

Data protection impact assessment (DPIA)

A DPIA[8] is a process designed to describe the processing of data, assess its necessity and proportionality, and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them. This covers, for example, processing large amounts of special categories of personal data, such as health data, data relating to disciplinary matters or data using profiling techniques, just to give a few examples. The DPIA process aims to provide assurance that controllers adequately address privacy and data protection risks of 'risky' processing operations. By providing a structured way of thinking about the risks to data subjects and how to mitigate them, DPIAs help organisations to comply with the requirement of 'data protection by design'.

Conducting a DPIA is a requirement of many data protection laws and, in such settings, is usually necessary for compliance with legal obligations. A DPIA is good practice,

8 See European Data Protection Board (EDPB, 2017), as well as UK Information Commissioner's Office (ICO, 2023) for more information.

irrespective of whether it is mandatory by law (Wagner et al., 2022). DPIAs are also important tools for accountability, as they demonstrate that appropriate measures have been taken to ensure compliance. In other words, a DPIA is a process for building and demonstrating compliance. The UK Information Commissioner's Office suggests a number of practical steps when conducting a DPIA (ICO, 2023).

Data protection impact assessment	Describes the processing of data, assesses its necessity and proportionality, and helps manage the risks to the rights and freedoms of natural persons, as well as determining the measures to address these risks.
Components Processing description	The purpose, nature, and scope of personal data processing needs to be identified, including which personal data is used and whether it falls into any special category.
Consultation process	Applicants, beneficiaries and their representatives, including registration officers, may need to be consulted to solicit their views on the necessity of data processing, the attendant risks, and the suitability of risk mitigation measures. Security and data protection experts should also be consulted to verify the suitability of the DPIA results.
Necessity and proportionality assessment	A determination that the processing activity is necessary and that the risks inherent in it are proportionate to the resulting benefits is a requirement for lawfulness.
Risk assessment	An evaluation of the likelihood and severity of each risk, and an assessment of the resulting overall risk level.
Risk mitigation	Measures to eliminate or reduce the risk, including the effect on and remaining level of risks.
Priority	Immediate

Logs, dashboards and monitoring

Automated, systematic monitoring of all data storage and processing activities is an essential component of data governance. The creation of audit trails for the collection, creation, and transformation of sensitive personal information is necessary to monitor data management and the various dimensions of data quality. Personal data protection rules require the supervision of data access, both of internal and external users, which is also necessary to oversee data sharing and service level agreements. For data security, it can highlight abnormal behaviour that requires further investigation and point to undue manipulation. Dashboards can help to monitor administrative processes, to ensure that they are working in line with regular system performance and provide a key tool for both day-to-day management and more general supervision by accountable parties. Barca et al. (2023a) highlight the potential of leveraging administrative data to increase social protection service quality, and Kent et al. (2006) describe how logs should be generated and used for monitoring.

Logs, dashboards and monitoring	Tools for the automated, systematic monitoring of all data storage and processing activities.
Components Logs	When data is stored and processed, a log that records its details (including e.g. a timestamp) should be created.
Dashboard	An automated process that retrieves logs over the reporting period and converts them into graphics that display relevant information in policy-relevant terms, for example, against appropriate benchmarks and with the right disaggregation (see Barca et al., 2023a). Examples of dashboard items are: number of newly assessed households, distribution of assessment outcomes for recently processed households versus historical averages, and number of failed scoring attempts due to missing data.
Reporting process	Responsibility for monitoring dashboards and reporting the insights on a regular basis must be assigned.
Priority	Intermediate

Use, sharing and publication

Note: The implementation mechanisms for this building block are covered in the Pillar 3: Access.

Archiving and deletion

The data management plan specifies the data lifecycle and, through an integral data retention schedule, prescribes how long data can and should be stored before it is archived, stored, or permanently destroyed. Using archiving software helps automatically move ageing data to the archives according to the retention schedule for each type of data. The sensitivity categorisation of data should be marked as their storage, archiving, and deletion might be subject to different rules and retention schedules on that basis. Archived data are indexed and have search capabilities, so that files can be located and retrieved when needed. The same software can erase data through the automation of periodically deleting unwanted or redundant data files, which helps maintain security compliance, save time and money, and mitigate the risk of data breach or leakage.

Data retention policy

The data retention policy determines how data is handled at the end of its lifecycle; deletion is the default, but some data should be archived at the end of the retention period. The prescription should be recorded in the data catalogue, and a regular process that implements deletion and archiving prescriptions instituted.

Data retention policy	Determines how data is handled at the end of its lifecycle.
Components Retention schedules	Each item in the data catalogue should be assigned a retention period. Once the period is over, the data should either be disposed of or archived. The schedules should be implemented automatically and take account of the data classification.
Archiving guidelines	A determination of which items are to be deleted at the end of the retention period, and which ones are to be moved into the data archive (see ▶ 'Data archive' section, directly below in Pillar 1).
Data disposal procedures	Simple disposal or deletion is insufficient, as data handled in that way can often be restored easily. Secure deletion, shredding of paper copies, and destruction of physical storage devices are examples of suitable approaches.
Priority	Intermediate

Data archive

A data archive is a secure data storage facility that preserves the data for occasional future retrieval for statistical, audit, forensic analysis or similar purposes. It keeps the data safe from unauthorised access while enabling legitimate occasional uses. The data to be stored in the archive is determined by the data retention policy (which is in turn informed by any laws rules and regulations that require continued storage for purposes, such as audits).

Data archive	A secure data storage facility.
Components Data storage	A dedicated server and storage media, or cloud storage, is the physical basis of the archive. Appropriate backups are similarly required.
Security	Appropriate security measures, in line with current ICT standards, should be followed.
Metadata management	The archive should not only include the original metadata that provides information about the stored information, but generate and store new metadata that determines the source of the data, the reason it was archived, who has accessed it for which purpose, and other relevant aspects.
Access policy	Guidance on the purposes for which data can be made available to specific actors.
Priority	Intermediate

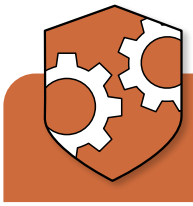


Table 2: LEVEL 1: **MANAGEMENT (Pillar 1)**

LEVEL 2: **Building block**	LEVEL 3: **Implementation mechanism**	LEVEL 4/5: **Roles and responsibilities**			
		Responsible	Accountable	Consulted	Informed
Planning	Data management plan	DA: compiles an overview of the data flow, processing activities, and management tools across the data lifecycle	GC: reviews and clears the plan	DP, DC, PA, IT: listed and other relevant stakeholders advise on and review aspects that apply to them	
Acquisition	Data acquisition policy	DA: proposes data acquisition policy, including policy objectives and details of the data to be collected	GC: reviews, amends and adopts policy proposals; sets SMART performance indicator targets	PA, DP, DC: provide inputs to policy formulation and review	
	Registration form design	DA: develops a registration form for piloting and, ultimately, adoption for primary data collection	GC: reviews and signs off on the form	DC: provides advice on registration form design; PA: communicates programmatic requirements	IT: receives data structure information to enable data-base preparation
	Data sharing agreements	DA, DP: agree terms and execute the agreement following GC clearance	GC: clears the agreement template and all particular agreements	IT: advises on technical and implementation requirements for automated data exchange	
	Service level agreements	DA, DP: agree terms and execute the agreement following GC clearance	GC: clears the agreement template and all particular agreements	IT: advises on technical and implementation requirements for automated data exchange	
Processing	Eligibility process documentation	DA: documents the PMT process for policy evaluation and replicability	GC: reviews the documentation to assess the suitability of the approach for sector policy objectives	PA, IT, DC, DP: provide guidance on aspects related to their activities	
	Eligibility determination	DA: generates PMT scores for registered households	GC: monitors actual PMT outcomes against expected ones and determines process changes where needed	IT, DC, DP: provide advice as required	PA: receives PMT scores

LEVEL 1: MANAGEMENT (Pillar 1)

LEVEL 2: Building block	LEVEL 3: Implementation mechanism	LEVEL 4/5: Roles and responsibilities			
		Responsible	Accountable	Consulted	Informed
Processing	Exit process	DA: updates PMT scores and identifies households dropping below the eligibility threshold	GC: monitors exit frequency and associated grievances, and adjusts policy where necessary		PA: receives list of households to notify of exit
	Logs, dashboards and monitoring	IT: generates dashboards on processing and data-related activities; DA: monitors dashboards	DA: provides dashboard specifications and ensures their continual fit with stakeholder needs	DC, DP, PA: advise on data and operational changes	GC, PA: monitor relevant dashboards
Analysis	Data catalogue	DA: compiles the catalogue and keeps it up to date	GC: uses the catalogue to monitor the scope of data collection and ensures that stakeholders provide updates	IT, DP, DC, PA: notify DA of catalogue-relevant changes	
	Data protection impact assessment (DPIA)	DA: produces a DPIA for the registry and its operations that takes other sector DPIAs into account	GC: reviews sector DPIAs, ensures that data collection and processing are appropriate and that risks are duly mitigated	PA, IT, DC, DP: provide DPIA to the DA and consider revising it in view of its DPIA	
Use, sharing and publication			[see Access Pillar]		
Archiving and deletion	Data retention policy	DA: formulates the policy; IT: implements automated storage, archiving and deletion in line with the policy	GC: clears the policy and reviews it periodically	PA: advises on related operational and compliance needs	
	Data archive	IT: operates the archive in line with the data retention policy	GC: monitors archive operations, availability and security		

Key: GC: data governance council, DA: database administrator, DC: data collector, DP: data provider, PA: program administrator, IT: IT services provider

Pillar 2: Quality

Data quality deals with procedures and processes that ensure data is accurate, consistent, complete, and reliable. The building blocks of data quality are the DAMA-DMBOK2 (DAMA, 2017) set of six dimensions: (i) completeness, (ii) accuracy, (iii) currency, (iv) consistency, (v) validity, and (vi) uniqueness. Data quality aspects may include accurate enumeration, data rectification, data quality assurance and control, and complete household listing. Data quality enables better eligibility determination, operational efficiency, and compliance, ultimately improving public satisfaction. Poor-quality data can lead to mistakes in beneficiary selection, attribution of the wrong benefit package, and dissatisfaction with public services.

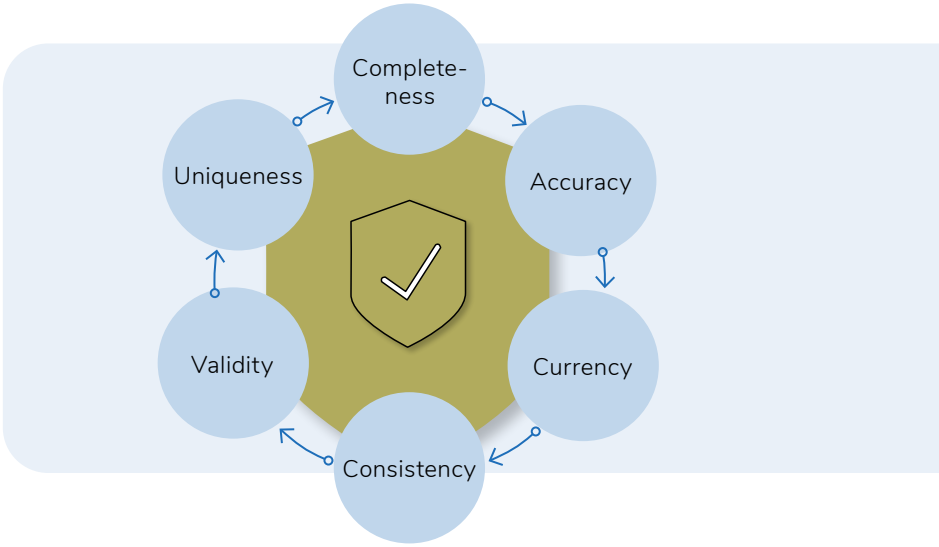


Figure 4. Dimensions of data quality

Source: DAMA-DMBOK2 (DAMA, 2017)

Completeness

Completeness is the extent to which all required data is present in a social protection database. Completeness ensures that all necessary information about individuals and households is captured, and that all households are recorded. Incomplete data can lead to the exclusion of eligible individuals from social protection programmes and to misguided decisions.

Relevance is the flipside of completeness. According to the data protection principle of data minimisation, only those data items that are required for legitimate and proportionate processing activities can be collected. Any superfluous collection exposes the registered population to unnecessary risk and imposes undue collection costs. The benefit of collecting each item of information needs to be weighed against the attendant costs and risks. A DPIA (see ▶ **section on 'Data protection impact assessment'** in Management Pillar) should both inform such an assessment and, in turn, be informed by it, as it affects the scope and volume of data collection. This aspect of completeness is also closely related to registration form design, which embodies the set of items chosen for collection.

Validation and reconciliation protocol

This protocol is a structured process used to validate the information in the social protection database on the basis of independent data sources and to reconcile it with administrative and survey sources. Both statistical validation and reconciliation with external sources support complete registration of the population, where this is an intended objective, although most systems do not aim for complete coverage. A data-informed deployment strategy that supports prioritisation at different levels is discussed in Barca et al. (2023b), and UNECE (2024) discusses how data integration strengthens statistical survey and administrative data.

Validation and reconciliation protocol	A structured process to validate and reconcile the information in the social protection database.
Components Census reconciliation	The census provides the most complete record of households in the period after its completion (with update cycles often lagging beyond the recommended 10 years in many low-income countries, with serious implications for data timeliness). The distribution of the population can be reconciled at small area level to ensure that the database captures all relevant settlements (it may also inform the next census sample frame). Here, as in the following points, a discrepancy between administrative or survey data and the social protection information should be investigated thoroughly until the source has been identified and the issue is either clarified or corrected.
Civil registration and vital statistics (CRVS) reconciliation	The official demographic record held in the CRVS is another source of information that aims for a complete account of the population, although this is often not the case in many low-middle income countries. Unlike the census, it draws on administrative data and is, thus, up to date at any moment.
Statistical validation via other sample surveys	National statistics agencies typically conduct a number of population sample surveys that can validate the sector databases by comparing survey estimates with registration data – noting there are sometimes valid reasons for discrepancies (e.g. prioritisation of coverage of vulnerable areas and groups). In addition, the sample survey often contains information on the receipt of social protection programmes, and can, therefore, function as a cross-check on the accuracy of eligibility determination and the effectiveness of social protection programmes.
Priority	Intermediate

Self-declaration

Options for households and individuals to register 'on demand' via digital channels, or perhaps forms submitted to public offices, often complement or replace enumerator-led intake and information updates. Such an approach allows households and individuals to provide registration data as far as possible, and provides a way to include previously unrecorded beneficiaries. For practical specifics, NIST (2017) provides help in its *Digital identity guidelines: Enrollment and identity proofing*.

Self-declaration	When a household or individual registers 'on demand' via digital channels or forms submitted to public offices.
Components Multi-channel engagement	The growing availability of smartphones and Internet access makes a digital portal where households can register themselves for programmes a potentially low-cost access modality for many digitally literate households. However, there are major constraints on digital access that many intended beneficiaries face, including device and telecommunications availability, literacy, and physical ability, which preclude a significant share of households from registering digitally. Alternative sign-up at accessible physical locations, such as local government offices, can overcome some of these barriers.[9] Forms and support for filling them out should be provided at these locations, which requires preparation and staff training.
Authentication	When beginning assisted registration in a digital or physical channel, a reliable and secure authentication modality is necessary to ensure that applicants are truly who they claim to be. Access to existing information, as per the next item, makes such authentication especially important for data protection. Registration officers also need to be authenticated for this reason.
Pre-populated information	Existing administrative data and previous survey answers can be provided for verification by households. The discrepancy resolution process (see ▶ section on 'Consistency' in this pillar) should be triggered in case of mismatches.
Physical verification	As registration can lead to valuable payments and services, verification of information accuracy is important and can be handled through physical verification. The use of pre-populated CAPI should facilitate this process (discussed in ▶ section on 'Consistency' in this pillar).
Priority	Intermediate

Accuracy

Accuracy refers to the correctness and precision of the data recorded in the social protection database. Accurate data ensures that the information about individuals and households reflects their true circumstances, and that eligibility determination can be conducted effectively on that basis. Inaccurate data can result in the misallocation of benefits, fraud, and errors in policy implementation, affecting the integrity of social protection programmes.

Registration officer training

Registration officer training equips the officers that collect household data with the instructions and knowledge required to perform their duties effectively. Training is especially important when non-professional enumerators carry out the data collection. The training is most directly linked with questionnaire design, but relates closely to data quality, data protection and privacy, and ICT security. For detailed guidance on survey-

9 The accessibility requirements set out in Annex I of the European Accessibility Act 2019/882 provide criteria for engagement channels that are suitable for all users.

type data collection, the World Bank's *Development Impact Monitoring and Evaluation (DIME)* has compiled recommendations for enumerator recruitment and training (World Bank, 2010; World Bank, 2022).

Registration officer training	Equips the officers who collect household data to perform their duties effectively.
Components General background	A general understanding of registration objectives and methodology provides a foundation for the registration officers to conduct their work appropriately.
Respondent handling	The solicitation of open and honest responses to personal and sensitive questions requires rapport building and preparedness for a variety of situations to foster a suitable environment. Basic interviewing techniques may be an important facet.
Questionnaire administration	A protocol for each item can be taught in the case of administered questionnaires. Apart from preparing enumerators for all the questions, they also need to be prepared for the survey app, including skip patterns etc. (as outlined under the ▶ sub-section on 'Pre-populated CAPI' in the section below on 'Consistency' in this pillar).
Data protection, privacy and security	Training on appropriate data handling, confidentiality, device security, authentication, and secure data transfers is necessary to implement data security in this first stage of the data lifecycle.
Mock interviews	A practical component in which enumerators apply the skills in a mock interview setting can provide helpful training and allow trainers to verify completion of the learning outcomes. Where possible, supervised field practice, in which enumerators conduct interviews with actual registration officers, is an effective final training stage.
Priority	Immediate

Pilot registration

A pilot registration drive, referred to as pre-testing (or preliminary testing) in the survey literature, is a small-scale, but nevertheless extensive, validation approach for data collection that can be employed for on-demand registration as well. It ensures that both survey instrument and enumerator training are effective at soliciting accurate information by trialling them under realistic conditions. In its Living Standards Measurement Survey guidance series, the World Bank (2010) offers advice on pre-testing and related topics. Note that even small-scale pilot registration is likely to collect sensitive personal data that requires protection, so that all appropriate measures should already be specified at this stage of the process.

Pilot registration	A small-scale, but extensive, validation approach for data collection.
Components Sampling strategy	The areas to test the survey should be sampled randomly, to ensure realistic conditions. In the absence of a clear strategy, convenient locations are likely to be chosen that are not representative of the overall environment.

Pilot registration	Testing cadre	The testing cadre are enumerators who are selected from the actual pool of volunteers. The set of roles to be tested should be extended to supervisors and managers, if applicable, especially if a training of trainers approach is used, to ensure that the entire system is functional.
	Feasibility assessment	The financial constraints on this large-scale continual data collection exercise make resource planning critically important. Apart from testing the enumeration and statistical aspects, the pre-test should be used to verify that the time per household and travel time between households allow the survey to be conducted on time and within budget.
	Feedback mechanism	A systematic approach to problem identification and procedure refinement that informs questionnaire design, CAPI implementation, and enumerator training should be developed as part of planning.
Priority		Intermediate

Real-time survey monitoring

Real-time survey monitoring is a supervision system that tracks and monitors responses as they are submitted by enumerators or applicants themselves. Although this may sound inapplicable in many settings, it is common practice for impact evaluations carried out in the most challenging of settings.[10] It supports data quality through the continuous quality assurance of data entry and supervision of enumerator performance. The monitoring system can be tested as a part of the pilot survey.

Real-time survey monitoring		A supervision system that tracks and monitors responses as they are submitted.
Components	Quality assurance	Quality assurance includes: (i) automated checks on data quality including consistency checks to verify that the data are in line with expectations and common sense, (ii) missing data monitoring, which tracks the prevalence of unanswered questions and the reasons for this, and (iii) outlier detection, which flags unusual entries. Quality assurance can flag issues at the question and registration point or registration officer level, allowing remedial action to be taken.
	Registration officer supervision	In addition to issues flagged by quality assurance tools, the supervision of activity levels (number of interviews undertaken, time per interview, etc.) can highlight problems at the enumerator and data collection area levels.
	Technical monitoring	High uptime and fault-free operation of the technical infrastructure is a condition for a well-functioning data collection system. Dashboards that monitor such metrics and that are reviewed regularly support this function.
Priority		Intermediate

10 J-Pal provides a ▶ guide to implementation and detailed procedures (Sachsse, n.d.).

Access and rectification modality

A data access and rectification modality is a mechanism for households to gain access to the data that the social protection database holds on them to rectify mistakes and fill in missing data. It supports overall accuracy, as households are the best source of information on their own circumstances. It aligns with statutory data protection rights and is, therefore, closely linked to the Security Pillar of data governance. Considerations on this topic can be found in the UK Information Commissioner's Office publication *Right to Rectification* (ICO, 2021b).

Access and rectification modality	A mechanism for households to rectify mistakes and fill in missing data.
Components Access modality	A reliable and authenticated way to access the information held by a social protection database on a household is the first main aspect. An online portal may be more user-friendly than an Unstructured Supplementary Service Data (USSD) solution, for those who can access it, but multiple modalities can coexist. It is important to offer access to the digitally excluded as well, which could be handled by assisted log-in at a public office, for example.
Rectification request mechanism	When a household discovers an inaccurate record, they may request that the information be corrected or 'rectified'.
Verification process	In some cases, documentary evidence could be used to verify the claim, in others it may trigger an enumerator visit to conduct physical verification. The rectification process should be recorded for each item in the corresponding data catalogue entry.
Updating process	Upon successful verification, the data may be updated within the social protection database. In cases where the information was provided by an administrative or private source, the discrepancy resolution process (see ▶ the section on 'Consistency' below in this pillar) needs to be triggered to ensure consistent and accurate information throughout the public sector and beyond, as provided for in the data sharing or service level agreement.
Priority	Intermediate

Currency

Currency is the degree to which data is up-to-date and available when needed. Timeliness in a social protection database means that the data is current and reflects the latest information about individuals and households, which is critical for informed eligibility decisions and the distribution of support. Outdated data can lead to delays in service delivery, incorrect eligibility assessments, and inefficient programme administration.

Data acquisition policy

See description of this item under Management Pillar.

Data sharing agreement

See description of this item under Management Pillar.

Service level agreement

See description of this item under Management Pillar.

Consistency

Consistency is the uniformity of the data across different records and databases. Consistency in a social protection database ensures that information about individuals and households is the same across different datasets and over time. Inconsistent data can lead to the duplication of records, confusion, and errors in benefit distribution, undermining the effectiveness of social protection programmes.

Pre-populated CAPI

CAPI stands for Computer-Assisted Personal Interviewing and refers to an electronic questionnaire implemented on a digital device, usually a tablet or smartphone. A pre-populated CAPI takes existing information to suggest answers for items that were previously recorded. CAPI supports efficiency and effectiveness by enhancing data quality, enabling flexible questionnaires that limit questions to relevant items, and allowing for real-time monitoring. It is closely related to various aspects of primary data acquisition and data quality. The idea of pre-populated information extends to self-declaration forms that applicants or existing beneficiaries complete themselves. Turkey's Integrated Social Assistance System (ISAS) deploys such an approach (World Bank, 2018).

Pre-populated CAPI	An electronic questionnaire implemented on a digital device that is pre-populated with suggested answers where existing data is available.
Components Pre-populated responses	A benefit of the interoperable nature of modern social registries is their access to extensive administrative data, which can be used to streamline the interview process. In particular, data items that are part of the questionnaire and which can be derived from an existing data source (possibly including a prior household questionnaire) should be included in the questionnaire as a suggested answer. The enumerator can then simply confirm this item, with a mechanism to mark discrepancies for reconciliation (also see ▶ **the next sub-section on 'Discrepancy resolution process'** directly below in this pillar).
Skip logic	Some information is only relevant for specific programmes, and some questions only apply to some households. For instance, questions about current schooling should only be limited to households with children. CAPI software facilitates implementation of such conditional questions.
Validity constraints	Digital data entry allows the responses to be limited to valid entries in terms of format and response range, such as only allowing dates of birth before a certain year for household members marked as children in the 'relation to head of household' question.
Priority	Intermediate

Discrepancy resolution process

A discrepancy resolution process is a set of procedures that aligns the original data sources with the most recent social protection database. The process enhances the consistency of data, and needs to be coordinated with external data access and manipulation, which are under the Access Pillar. The details, which may vary between different information items from the same source, should be specified in the data sharing agreement.

Discrepancy resolution process	A set of procedures that aligns the original data sources with the most recent social protection database to identify and resolve discrepancies.
Components Verification requirements	Most information items need to be verified in a distinct way. Using the data catalogue as a basis, a listing of how each item may be verified is necessary for efficient resolution.
Notification protocol	When two data sources diverge, deference to the master record is the default approach. Where there are grounds to believe that the master record is incorrect, for instance, due to an enumerator observation or a rectification request from a household, the verification requirements should be fulfilled to confirm the situation. The master record holder should then be notified about the particular changes that are required, so that the information can be updated accordingly.
Priority	Intermediate

Validity

Validity is the extent to which data accurately represents the intended measure or concept. Invalid data can lead to incorrect eligibility determinations, the misallocation of resources, and ineffective programme outcomes, compromising the goals of social protection initiatives.

Data catalogue

See description of this item under Management Pillar.

Data sharing agreement

See description of this item under Management Pillar.

Uniqueness

Uniqueness establishes an unambiguous representation of a social protection actor, such as a person, household, location, or programme, across the whole data system. It prevents duplicate records, ensures accurate analytics, and underpins fair and efficient service delivery. Uniqueness is enforced through unique identifiers and can be supported with data quality procedures such as matching algorithms for de-duplication.

Master data model

Master data can be summarised as essential information about the core components of a data system. It changes slowly, in contrast to transaction data, which evolves in daily operation. Accordingly, the master data model is a blueprint of the core entities and reference lists that underpin the data ecosystem. It establishes unique keys, standard attributes, and authoritative sources for each entity so that every system component refers to the same object in the same way. A well-structured master data model reduces duplication, enables interoperability, and is the foundation for data quality, as it facilitates deduplication, reconciliation, and analytics. The DAMA-DMBOK2 (DAMA, 2017) is an excellent reference on this topic, with an entire chapter on master data.

Master data model	Contains essential information about the core components of a data system.
Components Entity inventory	A complete list of 'master entities' (households, individuals, benefit programmes, payment cycles, geographic units, service providers, administrative areas) with plain language definitions.
Attribute schema	For each entity, the set of mandatory attributes (names, codes, dates, status flags) including data types, validation rules, and allowable value lists to ensure that the information is valid and consistent.
Relationships and cardinality	Diagrams and tables showing how entities link to one another (e.g. the individuals that make up a household, or the beneficiaries of a programme).
Master record	Identification of the authoritative source for each entity and attribute, plus rules for resolving conflicts (also see ▶ sub-section 'Discrepancy resolution process' in section on 'Consistency' above in this pillar).
Geographic master data	A standardised table of administrative divisions, localities, and perhaps Global Positioning System (GPS) coordinates in line with the address system.
Governance and stewardship	Assigned data owners who are responsible for updates and quality metrics, aligned with the data catalogue and discrepancy-resolution process.
Priority	Immediate

Unique identifier

A unique identifier (UID) is an alphanumeric code that is issued to each registration officer, whether household or individual, on first registration. As the name suggests, it serves as an identifier across databases in the social protection system, enabling data from different sources to be linked to the appropriate assistance unit. It also serves to establish identity by providing a link with hard-to-falsify verification information such as biometrics or log-in credentials. The master ledger of UIDs is highly sensitive and needs to be protected against loss, unauthorised access and improper manipulation. The World Bank has a number of publications on identity management, including its links to foundational national IDs, such as *Principles on Identification for Sustainable Development: Toward the Digital Age* (World Bank, 2017). It is worth noting that unique identifier information also constitutes personal data and, accordingly, needs to be protected by personal data protection rules.

Unique identifier	An alphanumeric code issued to a household or individual on first registration.
Components Secure, scalable and readable format	A sufficiently long, pseudo-random code that prevents revelation of sensitive information (such as area codes) and guessing attacks, and provides capacity for user population and coverage growth is needed. A checksum that detects data entry errors is also advisable, as is a human-readable format with separators, e.g. 1234-5678-9889.
Non-repeating codes	No identifier should be issued more than once to ensure its uniqueness, which is most easily accomplished by a central authority with a complete record of previously issued identifiers.
Separate individual codes	Where both individual- and household-level programmes exist, individuals should be issued with a separate individual code unrelated to that of the household. The household code can then be used as a relational attribute of the individual's record.
Reassignment rules	Household splits are a normal part of the lifecycle and need to be accommodated in the UID system. For example, in case of a split, the head of household may maintain the existing household code, but the split-off individual(s) need to either join an existing household or be issued a new household UID in case of household creation.
Robust issuance	Where possible, the code should be issued by a single institution to ensure uniqueness. In cases where connectivity to a central issuing authority cannot be guaranteed, robustness measures such as concurrency controls or pre-allocation pools are important. Deduplication and collision checks should be undertaken before final issuance is confirmed.
Priority	Immediate

Table 3: LEVEL 1: **QUALITY (Pillar 2)**

LEVEL 2: Building block	LEVEL 3: Implementation mechanism	LEVEL 4/5: Roles and responsibilities			
		Responsible	Accountable	Consulted	Informed
Completeness	Validation and reconciliation	DA: data administrator cross-references and reconciles newly collected and received data with existing entries and external sources	GC: monitors reconciliation and provides guidance where needed	DC, DP: provide data and clarify collection processes in case of reconciliation and validation issues	
	Self-declaration	IT: provides a digital channel for on-demand registration for all suitable programmes; DA: provides universal access to an alternative, non-digital registration channel	PA: determines registration requirements and information needs; monitors registration and availability and quality of registration channels, taking remedial action as required		
Accuracy	Registration officer training	DC: recruits suitable enumerators and trains them in skills including respondent handling, survey administration, and data protection, verifying learning via mock interviews	DC: monitors recruitment and training progress, taking remedial action as required	DA, PA: advise on the survey protocol	
	Pilot registration	DC: develops interview protocol, prepares data collection instrument, trains enumerator group, and tests it in various locations	DC: monitors data quality and requires instruments and protocol amendments until standards are met		
	Real-time monitoring	DC: conducts on-going quality assurance of data, field operations and technical infrastructure	DC: sets, monitors and enforces performance standards		DA, GC: receive regular updates on survey activities, outcomes and issues
	Access and rectification modality	DA, IT: provide an access portal, with reliable authentication, for applicants and beneficiaries to review, and possibly challenge, data held on them	DA: monitors access to the portal and the volume and outcomes of rectification requests, initiating remedial action as required for improving data quality		PA: informed in detail of relevant rectifications; GC: receives summary information about rectifications

LEVEL 1: QUALITY (Pillar 2)

LEVEL 2: Building block	LEVEL 3: Implementation mechanism	LEVEL 4/5: Roles and responsibilities			
		Responsible	Accountable	Consulted	Informed
Currency	Data acquisition policy	DA: proposes data acquisition policy, including policy objectives and details of the data to be collected	GC: reviews, amends and adopts policy proposals; sets SMART performance indicator targets	PA, DP, DC: provide inputs to policy formulation and review	
	Data sharing agreement	DA, DP: agree terms and execute the agreement following GC clearance	GC: clears the agreement template and all particular agreements	IT: advises on technical and implementation requirements for automated data exchange	
	Service level agreement	DA, DP: agree terms and execute the agreement following GC clearance	GC: clears the agreement template and all particular agreements	IT: advises on technical and implementation requirements for automated data exchange	
Consistency	Pre-populated CAPI	DC, IT: data collector and IT develop a CAPI app that downloads existing household information for planned visits, during which data is verified	DC: monitors quality of data received and performance of the CAPI app, including outages and other technical issues	DA: advises on the data verification and discrepancy resolution protocol	DA: receives reports on data discrepancies revealed during household verification
	Discrepancy resolution process	DA, DP, DC: jointly design and execute procedures for resolving discrepancies between primary and secondary data sources when they arise	GC: monitors the volume of and reasons for discrepancies, and initiates process remediation if required		
Validity	Data catalogue	DA: compiles the catalogue and keeps it up to date	GC: uses the catalogue to monitor the scope of data collection and ensures that stakeholders provide updates	IT, DP, DC, PA: notify DA of catalogue-relevant changes	
	Data sharing agreement	DA, DP: agree terms and execute the agreement following GC clearance	GC: clears the agreement template and all particular agreements	IT: advises on technical and implementation requirements for automated data exchange	

LEVEL 1: QUALITY (Pillar 2)

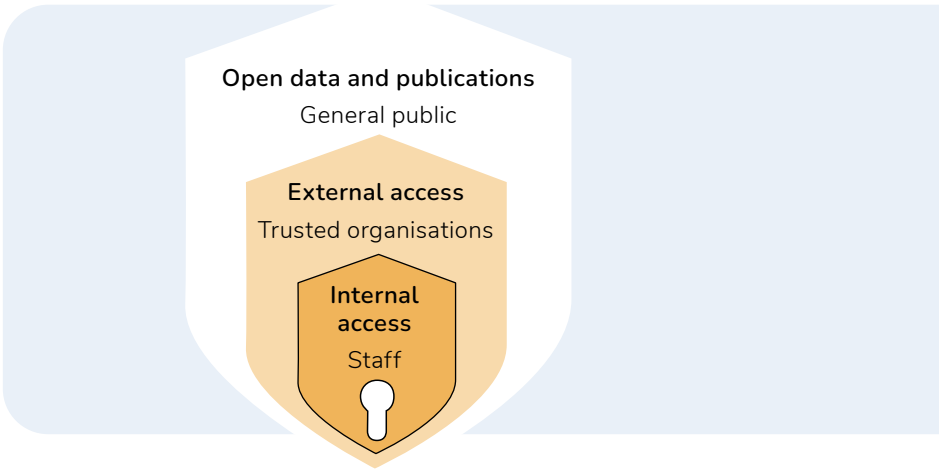
LEVEL 2: Building block	LEVEL 3: Implementation mechanism	LEVEL 4/5: Roles and responsibilities			
		Responsible	Accountable	Consulted	Informed
Uniqueness	Master data model	DA, IT: design and maintain the entity inventory, implement master schema, run quality checks and share logs for analysis	GC: endorses the model, allocates resources, and enforces compliance across all participating systems	DP, PA, DC: provide specifications, rules, and requirements to refine and validate the model	
	Unique identifier	IT: links with existing ID system; or creates sector-wide unique identifier	GC: determines registration officer identification policy to be followed across the system	PA, DA: advise on practical requirements for verification and operations	

Key: GC: data governance council, DA: database administrator, DC: data collector, DP: data provider, PA: program administrator, IT: IT services provider

Pillar 3: Access

The data Access Pillar focuses on policies and mechanisms to ensure that authorised users can efficiently retrieve and use data while maintaining data security, privacy, and compliance. At the building block level, the pillar categorises the different users or consumers of the data according to their respective relationship to the organisation: (i) internal users, (ii) external users, (iii) the general public, and (iv) general considerations, which cut across these groups. As social registries hold personal and sensitive data, key considerations such as referring to existing legislation around data privacy are explored under this pillar. Data access management also helps to contain possible data breaches, foster transparency, and empower staff and institutions to leverage data effectively.

Figure 5.
Types of data access



Internal access

Data access by staff is a condition for the effective execution of many duties and responsibilities. Providing access as and when required, at low administrative cost, while maintaining data protection and security, is the purpose of internal data access.

Human resources database

A HR database is the systematic assignment of access rights and is essential for the internal implementation of the data access policy. As per data protection rules, access to personal data should be restricted on the basis of the 'need to know' principle. Apart from the various HR management uses of such a database, perhaps the key function of an HR database from a data governance perspective is the assignment of job categories to each staff member. These groups, likely tied to the major job roles in the organisation, can be assigned user rights that satisfy the data requirements for the effective performance of each role (including both read and write access). As expressed in the data access policy, the default position should be no access, with rights only granted when

necessary. NIST (2024) proposes detailed technical controls for identity management that can serve as a reference for the following.

HR database	The systematic assignment of access rights for the internal implementation of the data access policy.
Components Job listing	A listing of job types in the organisation, with data requirements for each role. If a particular staff member requires data access that is not needed by all colleagues in the role, an internal data access request should be made, instead of adding the data access in general.
Access right assignment	Successively higher hurdles should be met for read access, followed by the right to change records, followed by the right to create new records and the right to delete existing records.
Principle of least privilege	This principle holds that users should be granted the minimum level of access required to fulfil their duties, and no more. In addition to limiting access to specific items, it should potentially be limited further by constraints such as particular geographies or times, to ensure that only strictly necessary data can be accessed. The definition of these variables should be drawn from the data catalogue to ensure alignment.
Priority	Intermediate

Account permission and revocation

Account permissions implement the access rights listed in the HR database and amended by successful data access requests. Each data system from which social protection information can be accessed must be restricted to permissioned accounts. To maintain data protection, the revocation of rights is as important as their granting. As in the prior point, NIST (2024) provides further specifics on account permissions in its AC-2.

Account permission and revocation	Implements the access rights listed in the HR database, as amended by successful data access requests.
Components Authentication	Authentication that meets the organisation's data security requirements is needed for each log-in.
Permissions	Permissions must include read access, write access, record creation and record deletion.
Process for adjusting user rights	The process through which a change in the HR database and a successful data access request triggers an adjustment of user rights.
Linked access rights	Access rights need to be linked with staffing information from human resources to ensure continued alignment, with job status changes triggering automatic adjustments to user rights. For instance, a person changing jobs in the organisation should be assigned the new job's profile according to the HR database, revoking previously granted access requests.

Expiring access rights	Access rights should expire automatically to prompt a fresh data access request.
Temporary revocation of access rights	A temporary revocation of access rights should be triggered by a violation of the data access policy, based on automated monitoring, while the issue is investigated.
Priority	Immediate

External access

In this context, external access refers to data access by organisations in the social protection space, as well as other social sector actors (e.g. health and education). These are likely to be public bodies, and the public sector is the focus of this first iteration of the Data Governance Framework. The initial focus is on laying a data governance foundation for members of the data governance council. It may be extended to non-governmental and international partner organisations, such as United Nations organisations, the World Bank and other multilateral development finance institutions, which would require adaptation of many of the tools, processes and procedures discussed below. Provision for private sector access is another possibility, which would require particular safeguards, starting with a new DPIA (see Management Pillar), as the two-way exchange of information with commercially-driven actors entails particular risks.

Data sharing agreement

See description of this item under 'Acquisition' in Management Pillar.

Discrepancy resolution process

See description of this item under Quality Pillar.

Secure sharing modality

When the legal, organisational and semantic conditions for data sharing have been met, the information needs to be exchanged via a secure and robust technical modality. Recent technical guidance provided by the UK's Government Digital Service (2025) gives details beyond the following points.

Secure sharing modality	A secure and robust technical modality for sharing information.
Components API integration	API integration that allows the recipient to transfer the latest data, as required, may be the most technically suitable solution in this context. A data warehouse provided by public IT services that stores the data and allows direct transfer is another suitable option.
Ad-hoc modalities	Ad-hoc modalities, such as use of a file transfer protocol or direct transfer via physical devices, are viable, but less suitable, options, as they entail a greater risk of security breaches and the more cumbersome process is likely to lead to less frequent data access, thereby working against the principles of interoperability.

Secure sharing modality	Up-to-date authentication	Authentication and other data security standards are clear pre-conditions here, as they are for all other digital aspects of the registry.
	Priority	Immediate

Open data/public access

Open data can provide information access to the general public, including academia, civil society, citizens, the media and policy analysts. In view of data protection requirements and a lack of direct regulatory control of standard-setting institutions, the level of detail of data that can be made available via such a modality is more limited, and anonymised, by necessity. Nevertheless, information provided via an open data platform can further the public interest and merits support and attention. Barca et al. (2023a) highlight the potential and importance of open data in social protection. For research and other public interest purposes, micro-data access is another possible modality, in which more detailed datasets are provided to vetted users, usually researchers, who need to follow strict data safekeeping mandates. The EU Data Governance Act (European Union, 2022) makes the case for this practice, which can promote socially beneficial data use, if handled appropriately.

Anonymisation process

Data held in a social protection database is inherently personal, sensitive and in need of privacy protection. As open data is available publicly without restrictions and identity verification, the publication of sensitive data would violate data protection laws. Accordingly, all individual or household-level data published under open access needs to be anonymised to remove identifiability. The European Data Protection Board (2014) gives technical advice on suitable anonymisation methods.

Anonymisation process		The process of anonymising individual or household-level data to remove identifiability.
Components	List of variables to be removed	A list of variables to be removed from all open data, particularly personal identifiers such as names, addresses, contact information, and physical characteristics etc.
	List of variables that can be published	The data catalogue's sensitivity classification can inform a listing of variables that can be published, with highly sensitive information potentially excluded from publication at any level of anonymisation and aggregation. Rare characteristics that can identify households or individuals, even in aggregated form, should be included in the list of sensitive items.
	List of variables that can be published as summary statistics	A list of variables that can only be published as summary statistics, such as averages or totals for some level of aggregation.

Anonymisation process	Definition of level of data aggregation for sensitive data	Definition of a suitable level of data aggregation for sensitive data to avoid identification via triangulation, including a minimum number of households to be included in each unit.
	Priority	Intermediate

Release approval process

Once data has been released to the public, its dissemination can no longer be controlled. In view of the irreversible nature of publication, it is essential that all datasets made available as open data be vetted carefully. A process similar to a data access request is indicated for this purpose. Guidance from California's Health and Human Services Agency (2021) outlines an approval procedure for sensitive data that can be adapted to the social protection setting.

Release approval process	The process of approving the release of data to the public.
Components Verification of non-sensitivity data	Verification of non-sensitivity and due anonymisation by reviewing the DPIA and data catalogue and seeking confirmation from a statistician that the dataset is sufficiently robust to triangulation to avoid revelation of sensitive personal information.
Data validation exercise	A data validation exercise that checks that the published data aligns with the original source in terms of accuracy, completeness and consistency is advisable.
Review of the meta-data	A review of the meta-data should ensure that the information provided about the data is accurate and clear.
Priority	Intermediate

Data portal

The premise of open data is easy, universal access. An online portal is a sharing modality that can provide such access. The US Office of Management and Budget (2013) provides specific guidance on open data and related sharing policies.

Data portal	A digital sharing modality that provides access to data.
Components Simple website for data downloads	Open data does not usually require user authentication. A simple website that provides for data downloads, for items that have passed the release approval process, is the core requirement.
Existing websites or portals	Instead of creating a site from scratch, which can be relatively costly, cumbersome and require scarce ICT resources, the data can be made available through existing websites or portals.
User accounts	If the data access policy permits provision of custom data sets (e.g. micro-data access) for requesting parties that have successfully completed a data access request, a website with user accounts through which the permissioned dataset can be downloaded can be a useful implementation aspect.
Priority	Intermediate

Cross-cutting items

Aspects of data access that apply across the three access types, including overall policy and processes that are necessary in a particular form in each case, are discussed here.

Data access policy

At its core, the data access policy determines who should gain which kind of data access to a given item. It draws on other aspects of data governance, such as the data sensitivity classification, and mandates the processes and procedures that facilitate implementation of its requirements. The policy should maintain a restrictive posture, meaning that the default is to assign zero rights to a role. Rights must only be assigned where necessary and the task cannot practically be performed by a role with existing rights. The more extensive the right is (read data < change data < create entries, delete entries), the higher the hurdle for assignment needs to be. NIST (2024) offers advice on the elements of access control in its control AC-1.

Data access policy	A document that determines who should gain which kind of data access to a given item.
Components Data access principles	A definition of data access principles provides general guidance for the policy itself and for staff in its application throughout the execution of their duties. This definition should include internal or staff access, the conditions under which data can be acquired and shared in the interest of furthering the institution's policy objectives, and the constraints under which data can be shared with non-public stakeholders, including the general public through open data.
Implementation aspects	The implementation aspects of the data access policy with regards to internal access (which are discussed below) include the monitoring system, data access control, and assignment of access rights and levels, including their linkage with authenticated IT accounts. These, like other implementation aspects, can be designed and documented within the policy.
External access	Implementation aspects of external access, i.e. within the public social protection system at this point, include specifications of data sharing agreements and data sharing modalities, and considerations regarding discrepancy resolution in cases where particular entries conflict.
Open data	Tasks towards making information available as open data include an anonymisation process, a release approval process, and details on the portal through which the data can be accessed publicly.
Review	The policy itself, the procedures that it mandates, and the data access in its various forms should be reviewed at set intervals, and changes made as deemed appropriate.
Priority	Intermediate

Access request processes

The data access policy can only provide general rules for granting access rights, and its restrictive posture means that many legitimate cases will be ruled out by default. To ensure due access, a request process that reviews cases and grants those that are in line with the general policy is required. Data access considerations vary according to the affiliation of the requesting party, being different for (i) the organisation's own staff, (ii) external access within the social protection space, and (iii) public access, including researchers, analysts, and the public sector. An example of a process for health data that can be adapted for social protection use is given by the National Institutes of Health (2023).

Access request process	A request process that reviews cases and grants those that are in line with the general data access policy and process.
Components Internal access	Internal access requests should be made via a form available to staff, for instance through an intranet or other resources that can be accessed via an authenticated user account. Form fields should include items such as the variables requested, the time and geographic extent of access, the rights requested (read, manipulate, create, delete), the system through which access should take place, and the rationale for the request.
Flow chart	A flow chart that would likely include approval by the line manager, review by senior staff, and implementation through account permissions can be formulated to create a standardised and efficient workflow that can be monitored effectively.
External access	External access by public bodies, likely to be from the social protection space, can be requested through a request form available on the organisation's website, or simply via an email. The request would likely be less structured, as the requesting party may not have detailed information. A short workflow is likely to be viable due to the number of such requests probably being limited. Creation of a data sharing agreement would follow successful completion of the preliminary stages.
Public access	Requests for public access, including open data, can be made via a form on the organisation's website. Details of the data requested, the requesting party's institutional or commercial affiliation, and the purpose of processing would be essential. An extract of the data access policy for open data and public access should be made available to allow requesting parties the opportunity to align with it. A flow chart that begins with the verification of categorical eligibility (e.g. the nature of the requesting party, the purpose of the request, and indications of likely adherence to data protection protocols), and that only proceeds if these are met, may be important to limit the workload imposed by such requests.
Sunset clause	A sunset clause should be instituted for all data access requests, to ensure that permissions remain relevant and necessary. A simplified extension process for internal access, and a provision for extension of external access via the data sharing agreement, can mitigate the administrative burden of this safeguard.
Priority	Intermediate

Consent management

Consent management is the end-to-end process of capturing, storing, updating, and enforcing data subjects' permissions for the collection, processing, and sharing of their personal data. It operationalises the principles of informed, specific, freely given, and revocable consent required by modern data-protection laws, and it provides auditable proof that data use remains lawful over time. The European Data Protection Board, EU Data protection authorities, and UK's Information Commissioner's Office (ICO, 2020) provide guidance on how to operationalise the following items in a real-world IT system.

Consent management	The end-to-end process of capturing, storing, updating, and enforcing data subjects' permissions for the collection, processing, and sharing of their personal data.
Components Consent registry	A secure database that records each consent event with the data subject's unique identifier, the scope of consent, a timestamp, potentially an expiry date, and evidence of signature or other acceptance.
Capture channels	Multi-channel tools, such as digital signature pads, USSD protocols, web portals, and paper forms, that attach consent to the relevant data.
Revocation and amendment	Both digital self-service and physical assisted avenues for beneficiaries to withdraw or change consent. This should trigger deletion of data held solely on the basis of consent, and other relevant actions including programme exit if necessary.
Audit trails	Data logs that show who accessed or modified consent records (see ▶ sub-section on 'Logs, dashboards and monitoring' in the Management Pillar).
Communication materials	Human-readable notices in suitable language(s) that are also appropriate for the applicant/beneficiaries' literacy level, possibly both in electronic and printed form, to provide lasting evidence, highlight revocation and amendment rights etc.
Priority	Immediate

Table 4: LEVEL 1: **ACCESS (Pillar 3)**

LEVEL 2: **Building block**	LEVEL 3: **Implementation mechanism**	LEVEL 4/5: **Roles and responsibilities**			
		Responsible	Accountable	Consulted	Informed
Internal access	HR database	DA: compiles the HR database according to stakeholder inputs	GC: reviews and signs off on the HR database	PA, DC, DP, IT: provide job listings with associated data access needs	
	Account permissions and revocation	IT: grants and withdraws access permissions in line with the HR database, and reports on permissions	GC: reviews access data and adjusts policy as required		
External access	Data sharing agreement	DA, DP: agree terms and execute the agreement following GC clearance	GC: clears the agreement template and all particular agreements	IT: advises on technical and implementation requirements for automated data exchange	
	Discrepancy resolution process	DA, DP, DC: jointly design and execute procedures for resolving discrepancies between primary and secondary data sources when they arise	GC: monitors the volume of and reasons for discrepancies, and initiates process remediation if required		
	Secure sharing modality	IT: implements the sharing modalities in line with access policies and data sharing, service level agreements, and reports data exchange metrics	GC: determines suitable sharing modalities, monitors exchanges, and adjusts specifications as required		
Open data	Anonymisation process	DA: develops the anonymisation process, including the data processing protocol; IT: implements technical aspects of the anonymisation protocol	GC: clears, reviews and monitors the anonymisation process	DC, DP, PA: confirm whether anonymisation of their data is sufficient	
	Release approval process	IT: provides data due to be uploaded to the portal; DA: clears data release	GC: gives clearance on the release approval process and monitors its implementation		

LEVEL 1: ACCESS (Pillar 3)

LEVEL 2: Building block	LEVEL 3: Implementation mechanism	LEVEL 4/5: Roles and responsibilities			
		Responsible	Accountable	Consulted	Informed
Open data	Data portal	IT: provides a digital open data portal and reports on usage	DA: specifies portal design and monitors usage		GC: receives reports on portal usage
Cross cutting	Data access policy	DA: formulates and maintains the data access policy	GC: reviews and signs off on the data access policy	PA, IT: provide guidance on operational data access needs	
	Access request process	IT: provides a digital access request form; DA: processes access requests	GC: reviews access decisions and amends policy as required	DP, DC, PA: advise on access policy and requests as required	DP, PA: receive information about access requests granted to data they provided
	Consent management	DA, IT: implement and operate the consent registry, and notice/receipt mechanisms; ensure withdrawal requests are acted on	GC: approves consent templates, monitors compliance metrics, and escalates breaches	DC, PA: propose the scope and granularity of consent; contribute to user design	DP, PA: kept up-to-date on consent-status changes to guide data processing and registration workflows

Key: GC: data governance council, DA: database administrator, DC: data collector, DP: data provider, PA: program administrator, IT: IT services provider

Pillar 4: Security

The data Security Pillar covers the measures and protocols implemented to protect data from unauthorised access, breaches, and other threats. Any technical processes employed to collect, process, store, use or share data should employ robust security mechanisms, for which threshold guidelines need to be defined. Data security has four building blocks, all referred to as 'measures' in accordance with the ISO 27000 standard.[11] They are distilled from: (i) technical measures, (ii) organisational measures, (iii) physical measures, and (iv) people measures. In many settings, public sector entities must comply with data protection and security standards, but further security and safety measures can be built to ensure that data security is instituted right from the design of technologies and processes to foster trust.

The core objectives of ICT security are to maintain the confidentiality of data and information, integrity of the data and operations, and availability of digital systems (NIST, 1996), and to ensure accessibility for persons with disabilities.[12] Confidentiality implies the preclusion of unauthorised access by internal and external actors. Integrity of data and operations arises from the avoidance of interference and manipulation. The availability of systems to authorised users is the result of continual accessibility, both to duly authenticated internal users and to the intended external users of the system.

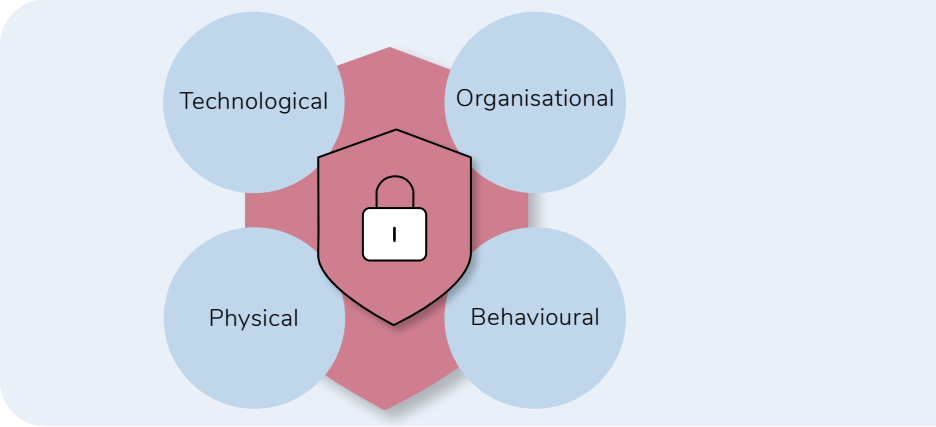


Figure 6. Types of ICT security measures

Source: ISO & IEC (2022)

11 For details on the standard, see: ISO & IEC (2022). An alternative, similarly authoritative listing of ICT security controls can be found in NIST (2020).

12 Accessibility for persons with disabilities can be ensured by complying with the accessibility requirements set in Annex I of the European Accessibility Act (European Union, 2019), to cite one regulatory example.

Building blocks and implementation mechanisms

The description of the Security Pillar's components is more concise than that for previous pillars. Informed by the ISO 2700 family of standards, it identifies technical, physical, organisational, and behavioural ('people') security as the major aspects of ICT security. The accounts of suggested implementation mechanisms are numerous and diverse, yet they are but a (salient) subset of ISO's 93 'controls'. Although security is a particularly extensive pillar, which requires efforts in multiple dimensions, it has been discussed elsewhere at length; hence, the synthesis of information that this Framework provides adds less value. Public sector ICT security strategies with their own requirements already exist in many policy settings, be it government-wide, sectoral, or institution-specific. Where these recommendations go beyond the existing requirements, they can be considered for adaptation to specific conditions. Additional considerations arise for general IT governance, such as those laid out in the ISO 38500 standard (ISO & IEC, 2024), but they are beyond the scope of this document.[13]

Settings where such a strategy is absent may be relatively low-capacity ICT operating environments in which general stipulations may be difficult to implement, and the necessary adjustments call for a substantial adaptation of the pillar anyway. In such a situation, the adaptation of ISO 27000 standards or a similar alternative (e.g. Swanson & Guttman, 1996; NIST, 2020) is recommended. Finally, ICT security is a fast-moving field that requires regular adaptation in response to technological developments and environmental shifts, rendering detailed suggestions prone to being outmoded rapidly. Accordingly, here, the discussion is limited to an abbreviated format in which pillar aspects take the place of mechanisms in receiving a short descriptive paragraph, followed by the mechanisms outlined as components.

Technical measures

Technical measures comprise technologies and protocols implemented to ensure the security and integrity of data within the social protection system. In the context of low- and middle-income countries (LMICs), these measures are critical for protecting sensitive information, preventing unauthorised access, and minimising the risk of data breaches. They encompass encryption, network security, data loss prevention, and more, which work together to safeguard the system from both internal and external threats.

13 Social security institutions that are members of the International Social Security Association (ISSA) are encouraged to access and approach ISSA for specific advice on *ISSA Guidelines: Information and Communication Technology* (ISSA, 2024), as they cover IT security and wider aspects of ICT governance and management.

Technical measures	Technologies and protocols implemented to ensure the security and integrity of data within the social protection system.
Components Encryption	Protects data by converting it into an unreadable format for users without a key, thus excluding unauthorised users. Data both at rest and in transit should be encrypted to ensure confidentiality and integrity, protecting it against easy interception.
Authentication	Verification of user identity is essential for security before access to the system and, thus, to sensitive data can be granted. Passwords, multi-factor authentication, and biometric methods are most used to limit access to sensitive data.
Data loss prevention	A set of tools and processes designed to ensure that sensitive data is not lost, misused, or accessed by unauthorised individuals, which includes the monitoring of data transfers, file sharing, and perhaps even printing to prevent data leaks.
Network security	The protection of network infrastructure from commercial and state hackers is essential for a large system that holds extensive personal data. Firewalls and intrusion detection systems can help to make sure that the social protection system's network is safeguarded against unauthorised access, hacking or malware.
Endpoint security	Security that relates to individual devices, e.g. laptops or mobile phones, that may access sensitive data.
Patches and updates	Regularly applying patches and updates to operating systems, software, and even hardware is key to closing vulnerabilities and enhancing overall security.
Priority	Immediate
Penetration testing	Simulates hacking attacks to test ICT security defences, with the aim of identifying potential vulnerabilities before they can be exploited by malicious actors. The test results should then inform security improvements and updates.
Priority	Intermediate

Organisational measures

Organisational measures include policies, protocols, and governance structures that establish clear roles and responsibilities for securing social protection data. These measures ensure that the institution has well-defined processes for managing security, responding to incidents, and continually improving practices to address emerging threats.

Organisational measures	Policies, protocols, and governance structures that establish clear roles and responsibilities for securing social protection data.
Components Incident response plans, disaster recovery and business continuity	Detailed plans need to be developed to handle security breaches, natural disasters, and technical failures. These plans outline steps for detecting, responding to, and recovering from incidents, ensuring minimal disruption to services and data integrity, and maintaining ongoing operations in emergency scenarios.

Organisational measures	IT supplier risk management	Identifies, assesses, and mitigates risks associated with third-party vendors or service providers. This includes ensuring that suppliers adhere to the same security standards and practices, as they can introduce vulnerabilities to the system through software, hardware, or outsourced services.
	Regular security review	Scheduled reviews of security policies, systems, and infrastructure to identify weaknesses and recommend improvements. This process may include audits, assessments, and testing to ensure continuous adaptation to new security threats and compliance with relevant regulations.
	Priority	Intermediate

Physical measures

Physical measures ensure the physical security of the facilities and hardware that store or access the social protection data. These protections aim to prevent unauthorised individuals from physically accessing, damaging, or stealing the hardware and storage devices that house sensitive information.

Physical measures	Measures that ensure the physical security of the facilities and hardware that store or access the social protection data.
Components Secure access	Involves restricting access to buildings, rooms, or areas where sensitive data is stored or processed. This can include access control mechanisms such as keycards, biometrics, or security personnel to ensure that only authorised individuals can physically interact with the system.
Device protection	Ensures that hardware devices used to access or store registry data are physically secure from theft, tampering, or damage. This could include locking mechanisms, surveillance, and other safeguards to protect servers, computers, and portable devices like laptops and smartphones.
Backup and recovery	Regularly creates secure backups of critical data and stores them in protected locations. These backups allow for the restoration of data in the event of data loss due to physical damage, corruption, or security incidents, ensuring that the registry's operations can continue without significant data loss.
Priority	Immediate

People measures

People measures address the human element of security, focusing on fostering a security-conscious culture within the organisation. These measures are essential for empowering staff and stakeholders with the knowledge and skills necessary to detect and prevent security breaches, both accidental and malicious.

People measures	Measures that address the human element of security, focusing on fostering a security-conscious culture within the organisation.
Components Training	Provides regular education for staff on security protocols, emerging threats, and best practices for data safekeeping. Training may cover topics such as recognising phishing attacks, using encryption, and adhering to data privacy laws, ensuring staff are aware of their roles in maintaining security.
Insider threat management	Monitors and mitigates risks posed by individuals working within the social protection sector who may compromise security, whether by design or by accident. This includes mechanisms for detecting suspicious behaviour, preventing misuse of access, and responding to potential internal threats.
Priority	Intermediate

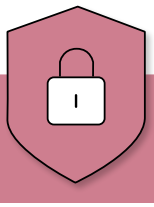


Table 5: LEVEL 1: **SECURITY (Pillar 4)**

LEVEL 2: **Building block**	LEVEL 3: **Implementation mechanism**	LEVEL 4/5: **Roles and responsibilities**			
		Responsible	Accountable	Consulted	Informed
Technical measures	Encryption	IT: ensures that sensitive social protection data are only stored in encrypted form, and that persons with direct data access follow data safety protocols while data is decrypted temporarily	IT: stipulates up-to-date encryption standards and policies, and monitors compliance		GC: notified of breaches of the encryption protocol
	Data loss prevention	IT: installs and maintains data loss monitoring and prevention systems	IT: specifies requirements for data loss prevention systems for all stakeholders, and monitors losses		GC: notified of data losses
	Authentication	IT: ensures that social protection databases can only be accessed by authenticated users from an authenticated system	IT: stipulates up-to-date authentication standards and policies, and monitors compliance		GC: notified of systematic authentication failures
	Network security	IT: implements security measures	IT: stipulates appropriate network security measures and monitors breaches and attempts		GC: notified of vulnerabilities, and attempted and actual breaches

LEVEL 1: SECURITY (Pillar 4)

LEVEL 2: Building block	LEVEL 3: Implementation mechanism	LEVEL 4/5: Roles and responsibilities			
		Responsible	Accountable	Consulted	Informed
Technical measures	Endpoint security	IT: implements security measures and monitors breaches and attempts	IT: stipulates appropriate endpoint security measures and monitors breaches and attempts, including in liaison with stakeholders that have bring your own device (BYOD) policies	DA, PA, DC: share information on the use of staff endpoint devices, including existing policies	GC: notified of systematic vulnerabilities, and attempted and actual breaches
	Patches and updates	IT: applies updates and patches systems as indicated	IT: determines update and patching schedule		
	Penetration testing	IT: contracts an external partner to conduct regular penetration testing	IT: determines testing requirements and sets contractual parameters		GC: notified of vulnerabilities
Organisational measures	Incident response plans, disaster recovery and business continuity	IT, DA, PA: the DA and PA develop plans with support from IT	GC: oversees sector-wide planning		
	IT supplier risk management	DA, DC, DP: institutions that hold registry data ensure IT supplier compliance with risk management procedures	GC: monitors due care in contracting and verifying compliance of IT suppliers	IT: provides guidance on procurement and contracting of reliable and honest IT suppliers	
	Regular security review	IT: comprehensively reviews IT security at each stakeholder institution and indicates required changes	GC: supervises the review process and ensures implementation of required changes	PA, DP, DC, DA: provide feedback on compliance, threats and breaches	
Physical measures	Secure access	DA, PA, DP, DC, IT: implement access security at all locations with sensitive data access	GC: provides guidance and monitors adherence		
	Device protection	DA, PA, DP, DC, IT: implements physical protection on all devices with sensitive data access	GC: provides guidance and monitors adherence		

LEVEL 1: SECURITY (Pillar 4)

LEVEL 2: Building block	LEVEL 3: Implementation mechanism	LEVEL 4/5: Roles and responsibilities			
		Responsible	Accountable	Consulted	Informed
Physical measures	Backup and recovery	IT: implements regular back-ups of all social protection databases, and formulates and tests recovery plans for cases of data loss	IT: determines back-up and restoration requirements	DA: provides guidance on required capac-ity and system requirements.	
People measures	Training	DA, PA, DP, DC, IT: train their staff on relevant aspects of ICT security and data protection	GC: provides training guidelines and moni-tors adherence		
	Insider threat management	DA, PA, DP, DC, IT: implement insider threat management mechanisms	GC: provides sec-tor-wide guidance on threat manage-ment approaches and monitors imple-mentation		

Key: GC: data governance council, DA: database administrator, DC: data collector, DP: data provider, PA: program administrator, IT: IT services provider

Part 3. Implementation guidance

Part 3. Implementation guidance

Across four pillars, this Framework suggests many steps towards good data governance. The steps are formulated in general terms that make no reference to specific conditions, as they aim to cover the essential ground, wherever they may be applied. Accordingly, the Framework gains universality at the cost of specificity. Even if one is to accept fully that the pillars and building blocks are suitable for the realisation of policy objectives, it needs to be determined whether the implementation mechanisms are the best approach for a given setting, and how to break these down into particular operational actions. This part suggests a **project management approach** to Framework implementation.

Implementation cycle

Although the Framework implies that data governance can be summarised, partitioned and assigned as proposed, many policy settings have a particular architecture that differs from that laid out in this Framework. Others will have already implemented some building blocks or find the particular mechanisms less than ideal for their policy environment. Instead of serving as a detailed guide, this Framework is a starting point for implementation planning. This part suggests a process that policy makers can use to **adjust, adapt, and operationalise the pillars** in a manner that is well-adjusted to their context. Figure 7 depicts the suggested process, which is based on Section 3 of NIST's Cybersecurity Framework 2.0 (NIST, 2024).

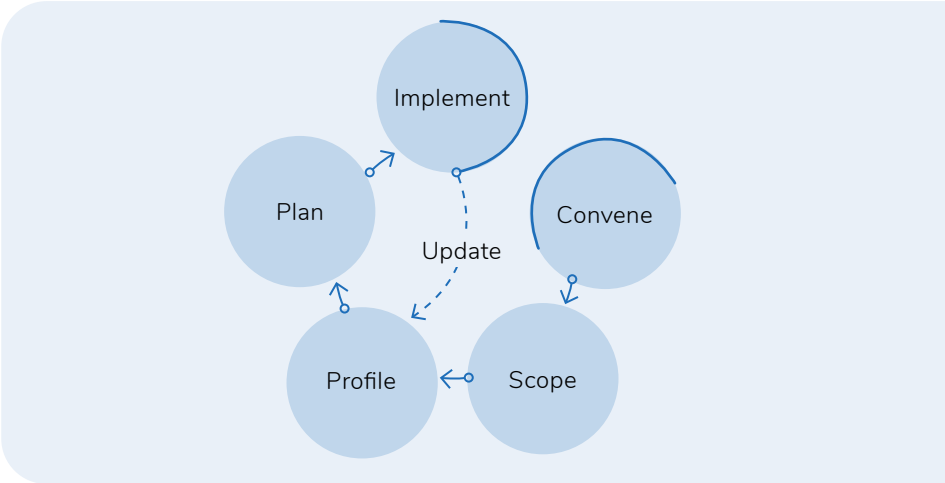


Figure 7. Data Governance Framework implementation cycle

The implementation cycle is presented in a structured and sequenced manner to describe the stages clearly. The reality of policy reform and implementation is much more adaptive and continuous than this 'linear cycle'; a responsive approach that is adaptive to evolving policy needs and stakeholder requirements should be embraced to ensure sustainable and well-adjusted policy outcomes. It is also important to note that many of the implementation mechanisms proposed in this Framework are on-going rather than once-off activities. For example, data access rights need to be set in line with job requirements and require immediate adjustment as staff transition to new roles or leave the organisation. Similarly, staff training needs to be conducted at regular intervals, data sharing agreements and service level agreements need to be adapted as circumstances evolve, policies require review, and ICT security must be kept up-to-date continuously, and so on. In short, the purpose of the implementation cycle is to build **dynamic, live systems**. The rest of this part discusses the steps involved, and we invite policy makers to consider them as part of the journey towards continuous improvement in data governance.

Step 1. Convene stakeholders: Governance and accountability

The previous parts of this Framework have highlighted not only the width and breadth of data governance as a field, but also the numerous actors who need to collaborate in its implementation. Intra- and inter-organisational effort is required for data governance to be effective, comprehensive and complete. A structured approach to fostering these efforts is a pre-condition for successful implementation and, thus, the first step in the implementation journey.

- **Map the data architecture:** A comprehensive **mapping of current (and potential future) data flows and responsibilities** can serve as the starting point. Compilation of a figure similar to the stylised Figure 7, but containing the full set of data providers and users, can be the heart of this task (also see **▶ the sub-section on the 'Master data model' in Pillar 2: Quality**). A listing of the relevant institutions that provide data-related governance, regulation and oversight may complete the picture. A digital infrastructure department that provides government IT services, a data protection authority that supervises the relevant law, an agency that oversees the implementation of ICT security standards, an institution with a sector-wide coordination mandate, and the finance ministry are examples of overarching stakeholders whose inclusion should be considered beyond the roles outlined in **▶ Part 1, Framework Overview**.

- **Gather stakeholders**: The gathering of core stakeholders is the first major step towards developing or strengthening a systemic and systematic data governance. An organisation with a coordination mandate for the sector or a top-level policy

coordination body such as the presidency in a presidential system are examples of institutions that may have the authority and status to convene other ministries, departments and agencies for a joint initiative. Although one institution has to issue the initial invite, framing the initiative as a collaborative effort is advisable, as effective implementation will rely on the commitment of multiple stakeholders. The creation of a **trusting and supportive environment** will be essential in this regard. An off-site venue may foster the desired atmosphere. The inclusion of high-level or more technical staff, and whether all stakeholders should be invited from the beginning or a focus on an initial core group is advisable, should be considered carefully.

- **Structure governance**: Data governance reforms are at least a medium-term process, if not a continual endeavour without a fixed end point. Such extensive, far-reaching, multi-stakeholder policy reforms require a strong governance structure to be sustainable. Two levels of organisation may be advisable. One is a senior-level **data governance council** that meets infrequently, but that convenes top-level decision makers of the key stakeholders whose role is to set strategic direction, approve initiatives, and monitor progress against set objectives. Ideally, it would be chaired by a high-level political patron with the ability to guide the agenda, mobilise resources, and adjudicate disagreements. The other is a **secretariat** that manages the technical, mid-level activities required to implement the Framework. The secretariat should be based within an institution at the centre of data flows, such as a social registry or social affairs ministry, giving it a clear view of requirements and the status of other stakeholders' progress, and be chaired by a senior manager.

Step 2.
Define scope of the Framework: Policy and contextual fit

- **Establish shared objectives**: The formulation of objectives shared by the various stakeholders in data governance for social protection sets the frame for subsequent activities. In line with the objective of establishing a collaborative and supportive group of partner organisations, **policy objectives** for data governance should be arrived at through a joint discussion in a forum open to all stakeholders. Examples of policy objectives are the creation of consistent data across all sector programmes, the creation of a more accessible data ecosystem,[14] the promotion of interoperability, stronger controls on third party service providers, and more uniform sectoral practices along the data lifecycle.

14 Including for persons with disabilities, by complying with the accessibility requirements such as those set out in Annex I of the European Accessibility Act Directive 2019/82.

- **Agree on general scope**: The general framework scope refers to the **relevant areas of the data governance framework** in terms of pillars, building blocks and mechanisms. It should reflect those parts of the general Framework outlined above that are necessary to implement the policy objectives identified in the previous step. Any that are missing need to be added, and those that are surplus to requirements can be eliminated. A Framework that is as small as possible, but as large as necessary, focuses resources and attention on the relevant aspects. For example, it may be the case that all building blocks of the ICT security policy and its implementation are handled by a specialised agency, in which case the security pillar could be dropped. In other settings, no household visits are conducted during registration and the corresponding building blocks can be dropped. An example of missing parts may arise from insufficient attention to any private sector provision that may be prevalent in a country, and which could require additional safeguards and coordination mechanisms.

- **Tailor the framework**: Having defined the general scope of the framework based on policy objectives, the third and final part of scoping is to determine **what applies at the organisational level**. For example, a data collection body, such as a national statistics agency that conducts 'survey sweep' registration drives, can implement real-time monitoring of data collection, whereas this mechanism would be of less relevance to an institution that provides social services.

Step 3. Profile organisations: Current status and gaps

- **Create profiles**: Planning for data governance reforms requires a clear understanding of the current organisational profile in terms of data governance. These profiles differ in outline and content across the sector stakeholders that engage with the data governance development process. Scoping in Step 2 will have revealed the framework components that apply, but the creation of a detailed organisational profile that documents all is likely to require inputs from colleagues. The first part of profiling each stakeholder organisation is to **gather the information** necessary for profile creation, and the second part is to **create the profile** that summarises the insights.

- **Identify gaps**: The formulation of development objectives can be framed as the difference between the status quo and desired situation. Whereas the creation of organisational profiles is a factual exercise, specifying the desired state is a matter of policy priorities in the context of the administrative, legal and political environment. In view of its current status, the organisation should **formulate a target** that at least meets minimum data governance requirements, if it currently falls below. When the basic conditions for sound data governance are in place, identification of possible improvements to the situation provides a policy target. Consultation of data maturity frameworks, such as the UK's Data Maturity Assessment for Government (HMG, 2023), can provide useful guidance in this regard, being careful to specify a realistically attainable improvement that can be implemented within the implementation cycles, which are discussed in the following Step 4.

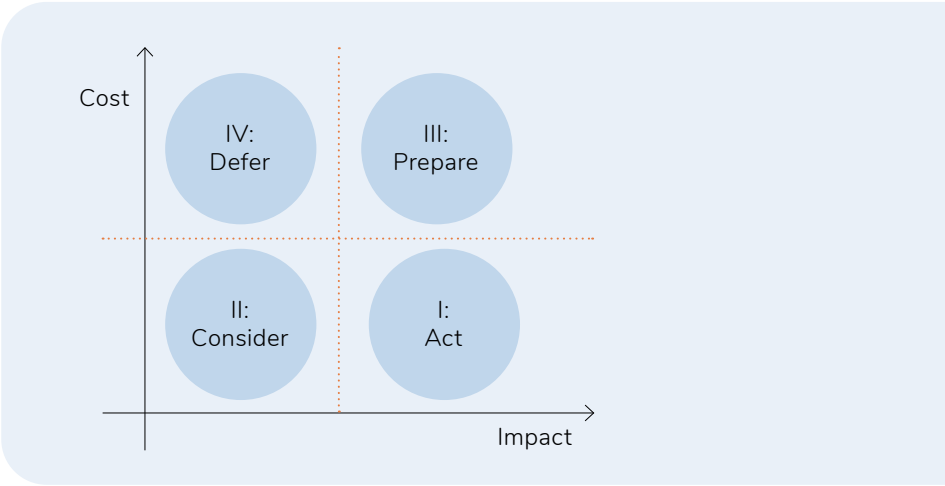
Step 4. Plan implementation: Prioritisation and project design

- **Evaluate impact**: Data governance activities are valuable because they ultimately support the policy outcomes that motivate social protection. The closing of any gap identified in Step 3 should have a beneficial impact, but in a world of limited resources, the question is *how much* impact. In view of their limited implementation capacity, policy makers need to choose between the options that their policy environment presents. An evaluation of their respective impact allows reform initiatives to be ranked to establish an importance hierarchy. There are many possible **dimensions of policy impact**, such as better service delivery, lower administrative cost, an enhanced beneficiary experience, or the avoidance of regulatory and reputational risk. Clear measurement or even estimation may not be feasible or may be impractical. For these reasons, thinking of impact as falling into a few categories, e.g. high/low, high/medium/low, or 1/2/3/4/5 should suffice for this exercise.

- **Estimate resource needs**: Resource needs are the flipside of policy impact. Just as the closing of relevant policy gaps should improve outcomes, it can consume **scarce resources** and, therefore, poses an opportunity cost of missed alternatives. Costs include items such as financial expenses, staff time, management attention, and infrastructure utilisation, and a broad categorisation that mirrors that of impact should suffice. Due to competing resource demands on each cost type, the reduction to a single cost category may need to be that of the highest scarce resource. For instance, high management attention (resource needs) can probably not be balanced by low financial cost, as fully occupied management attention becomes a bottleneck. The overall assessment of resources can be ranked similarly to impact, providing the other leg that prioritisation stands on.

- **Prioritise initiatives**: When impact and cost have been categorised, they can be plotted together in the manner illustrated in ▶ **Figure 8** for **resource-conscious prioritisation**. 'Broadly right, rather than precisely wrong' should be the motto, as this visual tool should facilitate rather than complicate the planning process. Initiatives in the quadrant marked I should be prioritised for immediate implementation, as they promise high impact at low cost. Low impact but low-cost initiatives in quadrant II should be considered for immediate implementation and selected if their implementation will not deter more valuable alternatives. Quadrant III contains the high impact and high-cost initiatives that need to be tackled, but which would detract from more efficient action in the short-term. Laying the ground for their implementation, which may lower cost or spread it over time, may be a sensible way to begin addressing these. Finally, quadrant IV includes costly, but low impact, items that should be deferred until their relative importance rises (as more high impact measures are exhausted) or their cost can be lowered.

Figure 8.
Prioritisation matrix



- Plan activities: A detailed implementation plan is the final preparatory activity after selection of the prioritised and costed activities. For each initiative, a review, adjustment or creation of an organisation-specific RACI matrix can be a first step. A more detailed development of tasks, their inter-relations and pre-conditions is advisable in this regard. Target dates for this personalised plan of action can then be set to create a Plan of Action and Milestones (POA&M) (OMB, 2001), for a light-weight monitoring tool, or a more extensive Gantt chart for a detailed project management approach. The secretariat should advise on the suitable tools and support planning, as required, and facilitate discussions on inter-dependent activities across organisations. Before adopting the various organisations' implementation plans, these should be validated, both at technical and leadership levels.

Step 5.
Implement the plan: Project management and iteration

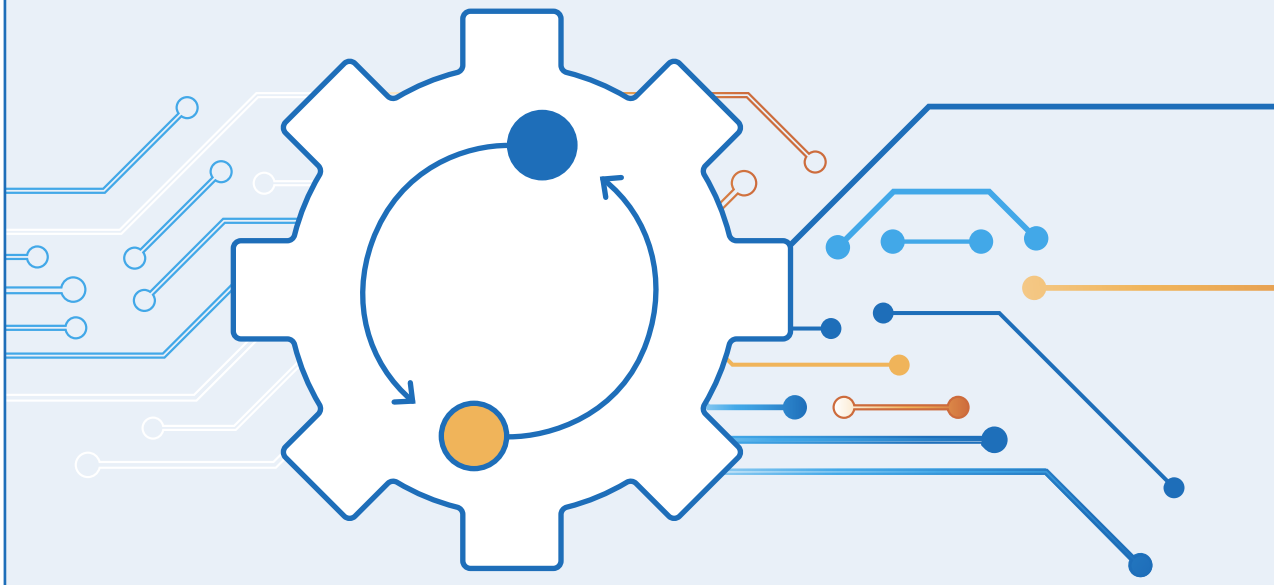
- Execute the plan: Careful scoping, profiling and planning exercises are the foundation of effective implementation. When those stages have been completed, it is time to convert well-laid plans into action. By this point, the core actors in each organisation should be aware of their position in the RACI matrix and their implementation responsibilities, the respective target dates for completion, and the resources needed for execution. Putting these resources to work should then turn policy intention into administrative reality.

- Account for progress: In view of the high impact of data governance on policy outcomes, the institutions that commit to developing their frameworks need to be held accountable. Open and transparent reporting of progress may be the simplest and most effective accountability mechanism. Mirroring the governance structure,

reporting can occur at different frequencies. Depending on the length of the overall implementation cycle, monthly or bi-monthly **technical meetings** at the technical level can be organised by the secretariat to gather status updates from all stakeholders. Quarterly **reports to the data governance council** that provide an overview of major developments and challenges may be appropriate. Bottlenecks that may be resolved by high-level interventions, e.g. resourcing or competency issues, can be addressed in this avenue.

- **Update profiles (refer to Step 3)**: On completion of each implementation cycle, all stakeholders should revisit their organisational profiles. **Updates to the current profile** show the evolution of data governance and provide a clear progress marker. A re-assessment of current status in areas untouched by reform initiatives is one side of this, and a **re-consideration of gaps** is the other. The latter is especially important, as it enables a maturity-style approach to continuous improvement that does justice to evolving data governance requirements and sets stretch targets for organisational capacity in this key area of modern public administration.

The iterative and recurring process outlined above provides practical advice towards implementing the Data Governance Framework summarised in ▶ Figure 1. The previous sections delved into the specific aspects and how it can be put in practice in general terms. The next part looks at some examples of how different countries have applied particular policy aspects of data governance in their contexts.



Part 4. Paths to data governance: Country cases

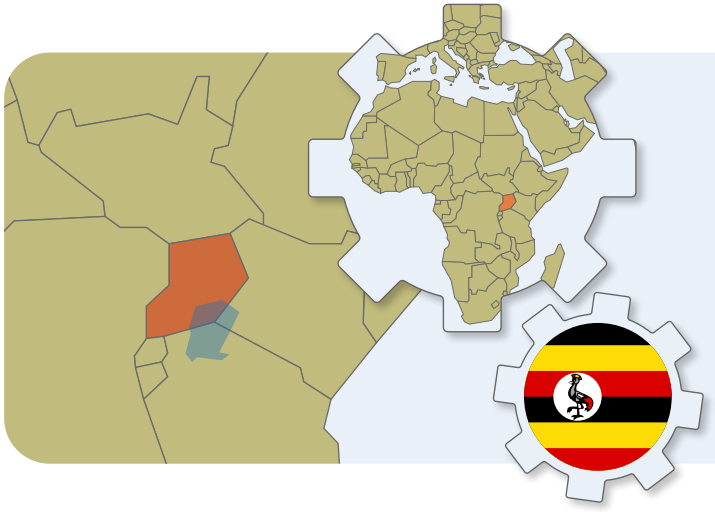
Part 4. Paths to data governance: Country cases

Policy implementation is a practical discipline that is best illustrated with real-world examples. This part highlights some of the steps that selected countries have taken, or are taking, in their data governance journey. The diversity of cases and stages of technical sophistication highlight that progress within the local context is what counts, that each country needs to find its own way on this policy path from where it finds itself at present, and that even the most progressive settings have ample space for policy development.

Uganda: Expanding social protection

Country profile

- Population 50.0 million (World Bank, 2025)
- Low-income country – Atlas USD 1,020 gross national income (GNI)/capita (World Bank, 2025)
- Size 241,038 km^2 (CIA, 2025)



Key social protection programmes

- Northern Uganda Social Action Fund (NUSAF) III – Originally aimed at areas devastated by civil war, the latest iteration of NUSAF provided poverty-targeted cash transfers and public works to approximately 600,000 households in rural districts.
- Social Assistance Grants for Empowerment (SAGE) – A bi-monthly social pension open to all older persons without a public pension, SAGE has around 300,000 beneficiaries.
- Public Sector Pension Scheme – Reaching roughly 275,000 pensioners in 2022, the public sector's role as largest formal employer makes this another key old-age support mechanism.

The issue

When the COVID-19 pandemic hit, Uganda reacted with vigorous lockdowns in many areas of life and the economy to protect population health. Although the government was able to shut down transport, schools and non-essential businesses, it faced a challenge in providing support to those most in need. The crisis revealed the uneven and limited coverage of social protection data as a systemic weakness that hampered the desired broad-based policy response. Apart from social pensions only being open to those 80 years old and above, the regional limitation of poverty-targeted cash transfers and public works to fewer than half the country's districts constrained the evidence base. The historically limited extent of social protection programmes, such as the absence of a social health insurance, did not allow the government to compile a wide-ranging list of households in need of crisis support.

The solution

The desire for a more flexible policy framework that can be leveraged in times of need has led the Ministry of Gender, Labour and Social Development to develop plans for a dynamic, interoperable social registry with national coverage. As the coordinating institution of the country's social protection sector, the Ministry will host a new integrated social and beneficiary registry, which will provide information to its own programmes, as well as those of other public institutions. A simultaneous expansion of social protection policy to provide a whole-lifecycle approach to supporting citizens through a widened set of risk will create the day-to-day demand for data that the system is due to generate. The necessary expansion of household registration inherent in this broadened interpretation of social protection will allow for greater shock-responsiveness, as it will capture more comprehensive information on needs and conditions than was previously the case.

Policy progress

Three core aspects are essential to put the vision of a dynamic, interoperable social registry in place. The first is a wide-ranging registration exercise, which is a challenge in a country without an extensive network of social service offices. A census-style survey sweep registration exercise will, therefore, need to be conducted as a first step. The Uganda Bureau of Statistics will provide support on the basis of a recent census that enables it to re-use the household roster, trained staff and digital data entry devices. Starting with districts currently covered by NUSAF, the first three years are expected to see data collection in 87 of Uganda's 144 districts, with the remainder following in the subsequent two years.

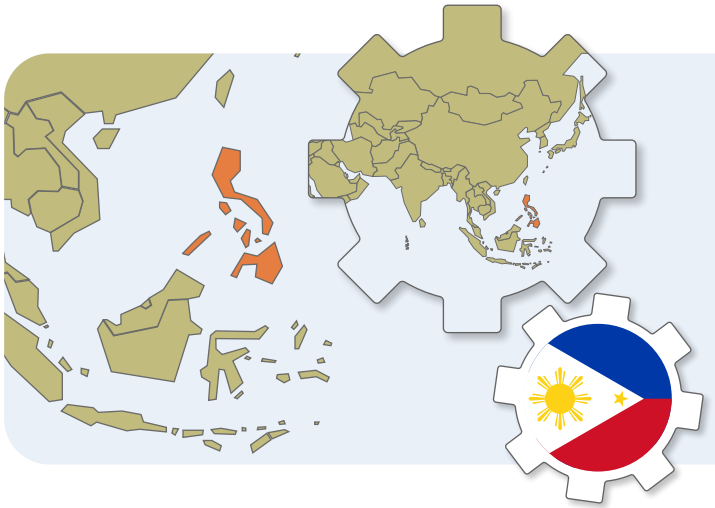
The second aspect will be the ability for households to register on-demand if they were not part of the initial registration, and to update information as required. Parish chiefs, who lead the second rung of the public administration structure, are envisaged to receive training and devices to provide this service to registrants. Beyond ad-hoc updates,

a 3-to-5-year cycle of large-scale re-certification surveys is currently envisaged. Automated updates of administrative data from other public bodies into the social protection system is the third component of the new information architecture. The Government Service Bus infrastructure provided by the National IT Authority will facilitate information exchange with key institutions, moving beyond existing integrations such as that with the Uganda Revenue Authority. Large-scale adoption of National Identity Numbers provides the person-level identifier that will link these sources to the new registry. When the system is complete, the combination of household-level data collection and the various administrative sources, including civil registration, will provide the country with the extensive national evidence needed for responsiveness to future shocks.

The Philippines: The road to interoperability

Country profile

- Population 115.8 million (2024, World Bank)
- Lower-middle-income country – Atlas USD 4,320 GNI/capita (World Bank, 2025)
- Size 300,000 km^2 (CIA, 2025)



Key social protection programmes

- Pantawid Pamilyang Pilipino Program (4Ps) – A conditional cash transfer, this flagship programme supports health, education and livelihoods of poor families.
- PhilHealth – A universal health insurance with subsidies for low-income households.
- TUPAD – An emergency employment programme that offers short-term for displaced and informal workers.

The issue

For many years, the Philippines depended on four yearly census sweeps[15] to populate social protection databases. However, households split, income levels fluctuated, and children outgrew eligibility long before new data was able to be collected. In addition, databases were fragmented, compounding data quality issues, with many programmes keeping their own beneficiary registers. During the COVID 19 pandemic this patchwork delayed the provision of emergency cash and magnified targeting errors. Inconsistent structures and a baseline 'repeatable' data maturity rating suggests that many data governance processes remained ad hoc, exposing funds to leakages and beneficiaries to delays (DSWD, 2025).

The solution

The Department of Social Welfare and Development (DSWD) is replacing its data collection through an interoperable data exchange system with the Community Based Monitoring System (CMBS) spearheaded by the Philippines Statistics Authority (PSA). DSWD constructed a dynamic social registry managed by the Social Registry Office, guided by DSWD's new Data Governance Framework (DSWD, 2025). Households can update their own records or do so through social workers between survey rounds through i-Registro. An API gateway lets authorised agencies exchange data in real time; a master data service tied to National ID PhilSys numbers reduces duplication and surfaces inconsistencies. A consent module limits each agency to only the fields its mandate requires, and automated quality tools backed by a metadata registry enforce DAMA DMBOK standards across the data lifecycle. The framework assigns clear roles to a Data Governance Council, Technical Working Group and operational stewards, mandates maturity assessments and audits, and embeds privacy and security controls into every stage of collection, storage, use and disposal.

Policy progress

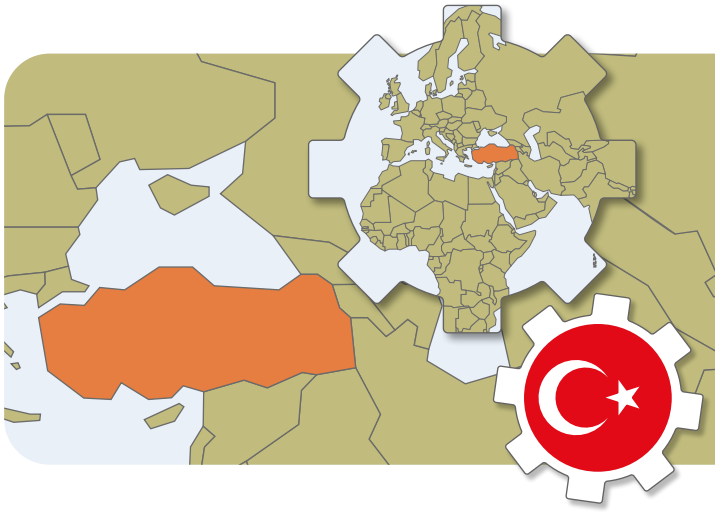
The COVID-19 experience triggered a push for integration, reinforced by the creation of a Social Registry Office to spearhead reforms. Pilots of i-Registro in several municipalities already validated and shared beneficiary data in real time. Current priorities include linking tax, pension and education datasets through the API gateway, finalising a national data dictionary and metadata registry, and launching a consent updating service so citizens can manage cross agency sharing. Regular maturity assessments, compliance audits and staff training are conducted to build a culture of evidence driven decision making. As these elements converge, the shift from fragmented, outdated records to a governed, interoperable data ecosystem is underway to shorten enrolment times, reduce duplication, and deliver support that is targeted more effectively.

15 Data collection was referred to as Listahanan initially, then became the Community Based Monitoring System.

Türkiye: Approach to dynamic data

Country profile

- Population 85.5 million (World Bank, 2025)
- Upper middle-income country – Atlas USD 11,730 GNI/capita (World Bank, 2025)
- Size 783,562 km^2 (CIA, 2025)



Key social protection programmes

- General Health Insurance – universal social health insurance, universal coverage
- Emergency Social Safety Net – unconditional cash (humanitarian), 1.5 million refugees
- Conditional Cash Transfer Program, Disability and Elderly Pensions, and Birth Assistance Programmes – among the basic social protection (non-contributory payments) programmes in Türkiye, covering 5.4 million people
- Türkiye Aile Destek Programı (Family Support Program) – unconditional cash transfer for low income households, 3.6 million households assisted in 2024

The issue

The estimation of economic welfare through a proxy means test requires a considerable amount of household data, which used to be collected in Türkiye through large-scale surveys. The great logistical challenges of such extensive surveys, comparable only to a census, meant that they would only be conducted every few years. But households' living conditions can change quickly, as studies of poverty dynamics show. As a result, the assessed and actual conditions can diverge, leading to the misallocation of poverty-targeted benefits over time, as some households' needs grow while the conditions of others improve without a reduction in their receipt of benefits.

Another complication is that newly created households, e.g. those established by young adults, may not be captured in the system at all. Finally, the intended support programmes or benefit packages may evolve due to changes in other data, such as household demographics for categorical programmes or location for geographically targeted ones. In short, a static assessment approach is not able to do justice to the dynamic nature of people's living conditions, whereas a more responsive system may

mitigate the issue. One of the big challenges in the Turkish social protection system is to effectively combine social services and employment policies with the social assistance system in order to increase the impact of social protection policies on poverty alleviation programmes, to make it more likely that support will only be needed temporarily.

The solution

Türkiye has taken several steps towards dynamic social protection data. A new approach was developed starting in 2011 with the creation of the Integrated Social Assistance System (ISAS) social registry. This has grown to combine administrative data with household interviews, also using active outreach and local information to complement the data collection system. Household visits are now conducted by local social assistance investigation officers, who get to know their clients over time. Visits to update information are done at least once a year, rather than on a multi-year schedule. The shift to local data collectors has also facilitated on-demand registration, which enables new households or those whose circumstances have changed to be considered.

The other main reform initiative was to connect numerous administrative databases to the social protection system and to store key information items in a social registry. As documented in a report on the ISAS (World Bank, 2018), Türkiye embarked on a multi-year project to connect all relevant public institutions that hold social protection data through data systems that would exchange data automatically through APIs. Administrative data is the basis of much of the socio-economic data on households in the ISAS. The main purpose of household visits is to verify the household situation by comparing it with the data in official records. In this way, inclusion and exclusion errors are reduced and public resources used more effectively and fairly. At the same time, household visits ensure that individuals receiving assistance are seen as people with needs, not just as data. In this respect, household visits both strengthen the humanitarian dimension of the social assistance process and ensure continuous communication with those in need. Secure tablet applications used by foundation staff during field visits make the process more digital, reliable and faster, thus making a significant contribution to the dynamism of social assistance.

The data collected in this way, such as demographic information from civil registration or asset ownership from vehicle and land registries, feeds directly into the social assistance and benefits assessment process. Moreover, the digitally collected data is integrated with the personalised process of household visits by pre-populating forms and verifying important changes with programmatic implications, such as those requiring exit or calling for active outreach as new data for a household suggests an expansion of eligibility to other programmes.

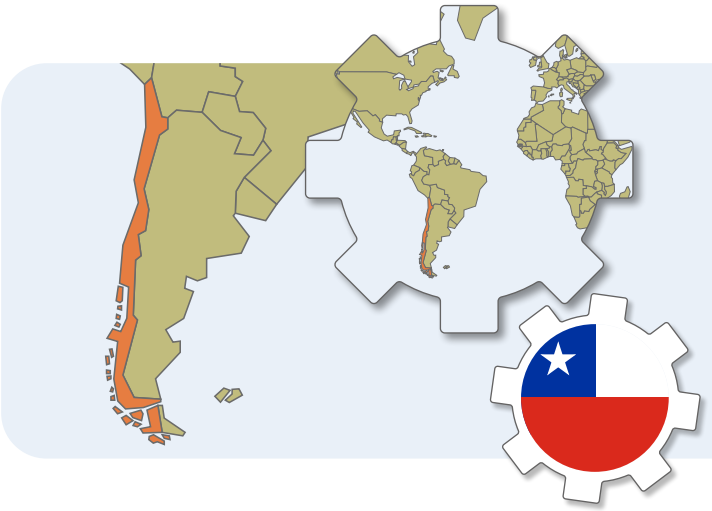
Policy progress

After more than a decade of system development, Türkiye now has a mixed system of household visits and interoperable administrative data that is a prime example of policy dynamism through integrated data collection. Currently, 29 institutions and over 120 databases are connected to the interoperable system. Additionally, around 9,000 social workers working in roughly 1,003 offices visit their clients frequently to maintain accurate data on other household characteristics. The social assistance investigation officers confirm important updates, conduct active outreach, and can also rectify information in a two-way information flow. Further advances in the system would lie in moving from the current proxy means test approach to a fully means tested assessment approach of economic conditions. However, such a shift would require structural changes in public administration and perhaps even economic activity, meaning that they lie beyond the remit of social protection. Developing and strengthening interoperability among social services, employment and social assistance policies at legal, digital, programmatic, and institutional (for both central and local basis) levels is needed to progress poverty alleviation policies further. Towards this, reforms have already started, and more development is planned.

Chile: 'Only ask once' policy

Country profile

- Population 19.8 million (World Bank, 2025)
- High-income country – Atlas USD15,800 GNI/capita (World Bank, 2025)
- Size 756,102 km^2 (CIA, 2025)



Key social protection programmes

- Fonasa – social health insurance, 78 % of residents covered
- Pensión Garantizada Universal – non-contributory old age pension, approximately 2.4 million > 65-year-olds covered
- Subsidio Familiar Automático – child allowance/conditional cash transfer, approximately 400,000 children covered

The issue

The repeated collection of similar data led to a number of problems in Chile's social protection system. One was that similar information could be collected in varying formats, leading to incompatible information. The collection of age versus date of birth is one example, potentially leading to discrepancies over time as the two items may differ for up to a year in the case of age-based eligibility. As each collection entails a risk of error, repeated collection also increases the risk of inaccuracies, even if the formats are the same. Moreover, changeable data items require updating, and data held in multiple places raises the likelihood of data becoming outdated if updates fail to reach all databases. In sum, repeated collection of similar data raises the risk of discrepancies and inaccuracies across the system.

The implications of this for registered persons and beneficiaries are considerable. Perhaps most importantly, inaccurate data may lead to undue refusal of benefit provision, or the provision of incorrect services or benefit packages. Data provision costs also increase, particularly for items that require documentation or physical verification. Similarly, data update and rectification efforts are increased with each point of collection. Fortunately, a seemingly simple solution can address these issues.

The solution

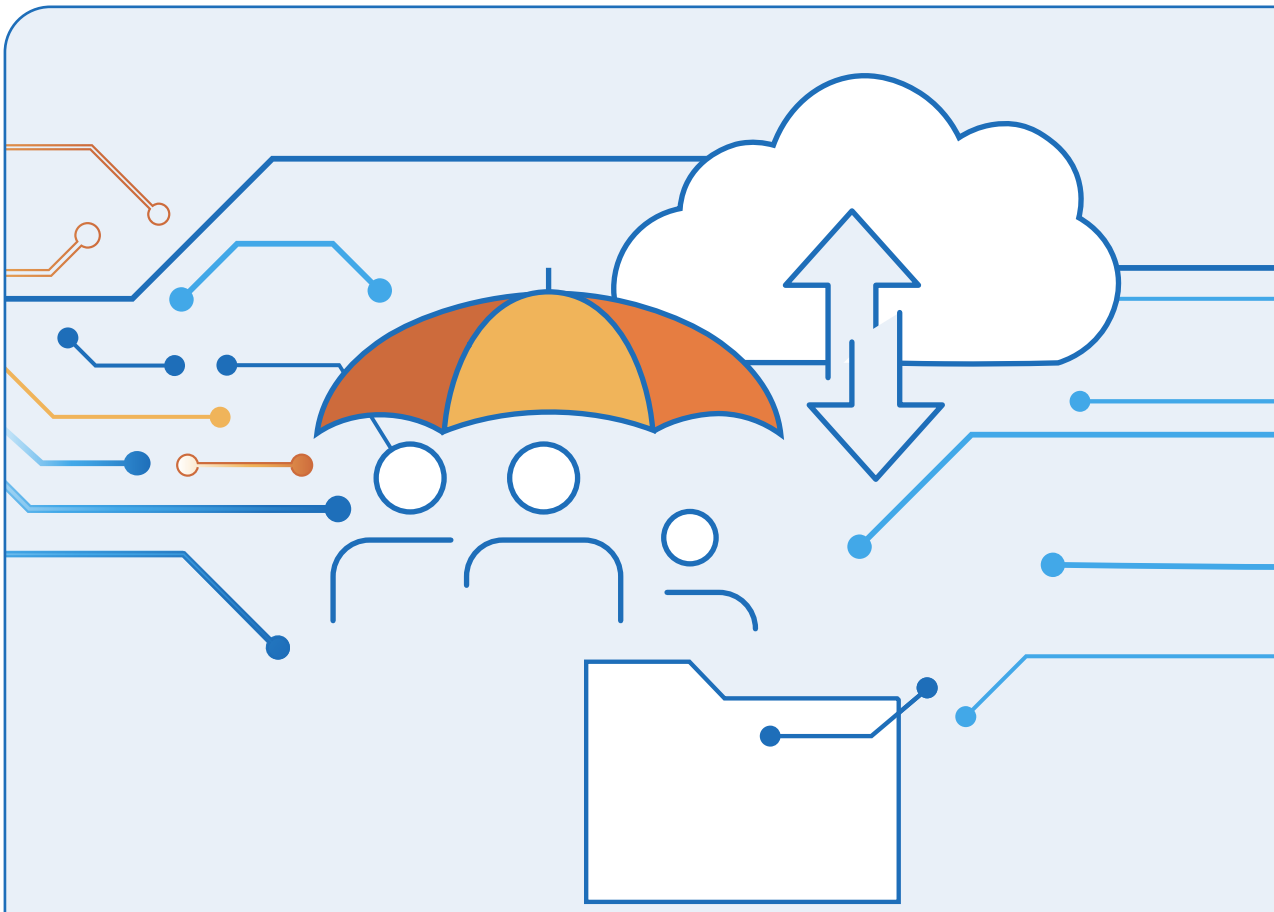
'Only ask once' is the paradigm Chile's government has adopted. The concept of a single source of truth for each data item is a closely related one: all information should have a well-defined origin that serves as the reference for its use within a system. When data is captured from citizens, it is stored in a clearly defined place that users with appropriate access rights can query for their particular purpose. It is only permissible to ask for the data if it is unavailable from its assigned source of truth database.

Although the idea is simple, its implementation imposes considerable demands. A central data catalogue that defines all available data, its storage, and the conditions under which it can be accessed is one aspect. A data transmission system that enables access as required, but does so in a secure manner that verifies credentials, is another. Thirdly, data transmission must be two-way in case the data has not yet been captured and needs to be committed to storage. Finally, a clear data rectification approach that determines how incorrect or outdated information can be revised and transmitted to enter the single source of truth needs to be formulated. For the maxim to become a reality, all institutions that wish to process citizen data need to use and contribute to this data system.

Policy progress

In Chile's exemplary case, 'Only ask once' is not merely a good intention, but a nationwide policy for government institutions. Although it is not a component of the new data protection law (Digital Transformation Law 21.719 passed in December 2024), it has

already became government policy. However, practical implementation required a phase-in that is now gathering pace. Use in social protection is most evident in the launch of the Ventanilla Unica Social, or 'Social One-stop Shop', which brings together 130 procedures and services from various public institutions in one (digital) place. Substantial efforts have, thus, been made by these actors to harmonise their ICT systems, resulting in a lower burden on citizens, higher data quality, and an increase in service quality due to more dynamic and accurate databases. An expansion to the municipal level, which integrates the social registry with the municipal management system and that implements a large number of relatively small social protection programmes, occurred in 2025. This enables municipalities to record and manage social cases as well as assign social benefits, improving services for individuals who prefer or require assisted attention rather than self-service and facilitating the work of public officials by integrating the multiple platforms they previously needed to manage cases. These impressive reforms illustrate how a simple data governance idea can have profound implications across an entire country.



Concluding remarks

Concluding remarks

In striving for an accurate, fair, and user-friendly information system, data governance touches on a remarkably diverse range of policy questions. In an effort to move beyond general exhortations on good practice, this Framework proposes numerous implementation mechanisms across four pillars of data governance. As a number of these mechanisms need to be replicated by multiple stakeholders, a substantial resource commitment is required across the social protection sector to achieve good data governance. The reward of more responsive, reliable, and secure service delivery should make the investment worthwhile.

Although this Framework outlines a roadmap towards operationalisation, it is far from a detailed plan of action. Instead, it serves as a starting point for a social protection sector that wishes to build its governance standards. Adaptation to local conditions and the specification of detailed tasks are where the real work starts. Identification of superfluous parts, addition of missing components, adjustment to the policy context, and alignment with existing initiatives rules and regulations will go a long way towards putting a universal framework into terms that are relevant to a given country setting.

The institutional architecture of social protection sectors differs as widely as the programmatic scope of programmes. As such, careful consideration of the required data governance aspects goes beyond mechanism to the Framework's overall scope. Other policy designs than are implicit in this exposition will require adjustments, but the general principles of data governance, and even the bulk of implementation mechanisms, should be relevant across the diversity of real-world policy settings.

Although this document provides a starting point for a journey towards good data governance, the search for a conclusive endpoint would be a mirage. In the time it takes to implement a tailored version of this Framework, our conception of data governance may already have evolved to keep pace with developments in technology, policy, and society. Moving all institutions of the social protection sector onto a uniform compliance level would be challenging, and a data maturity approach may be a constructive recognition of the varying levels of capacity. And even for the most compliant institutions, such a maturity approach is an acknowledgement that continual adjustment and development are required to achieve – and maintain – good data governance in an evolving world. If this Framework can catalyse such a journey in even just one setting, then it will have achieved its objective of fostering good data for effective universal social protection.

References

Essential background reading and further details on the topics covered in this publication that the interested reader may wish to consult can be found in the following references:

Barca, V., Hebbar, M., Knox-Vydmanov, C., and Brzezinska, I., *We have the data, let's use it better – Pushing the boundaries of administrative data analysis and use*, GIZ, 2023a

Barca, V., Kreidler, C., Silva Leander, S., Ouedraogo, S., Blundo, L., Beazley, R., and Ocampo, A., *The challenge of coordination and inclusion: Use of social registries and broader social protection information systems for capturing multiple vulnerabilities in West Africa* (Regional Synthesis Report), WFP and UNICEF, 2023b ▶

Broadband Commission, *Data governance toolkit: Navigating data in the digital age*, 2025 ▶

California Health and Human Services Agency (CHHS), *Data de-identification and data discovery guide*, CHHS, 2021

CIA, The World Factbook [online], CIA.gov, 2025 ▶

CORE-MIS, CoreMIS Wiki [online], 2025 ▶

Data Management (DAMA) International, *The DAMA guide to the data management body of knowledge (DAMA-DMBOK2)*, (2nd edition), DAMA International, 2017

Department of Social Welfare and Development (DSWD) of the Republic of the Philippines, *Administrative Order No. 02*, DSWD, 2025

Digital Principles Working Group, Principles for digital development (Version updated) [online], Digitalprinciples.org, 2024 ▶

Enqvist, L., Striking the balance: Preserving individuality in the era of highly structured data collection in automated social security case administration, *European Journal of Law and Technology, 14*(3), 2023 ▶

European Data Protection Board (EDPB), *Opinion 05/2014 on anonymisation techniques*, EDPB, 2014 ▶

European Data Protection Board (EDPB), *Guidelines on data protection impact assessment (DPIA)*, EDPB, 2017 ▶

European Union, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, Official Journal of the European Union, 2016 ▶

European Union, *Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services*, Official Journal of the European Union, 2019 ▶

European Union, *Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)*, Official Journal of the European Union, 2022 ▶

Faundeen, J. L., Burley, T. E., Carlino, J. A., Govoni, D. L., Henkel, H. S., Holl, S. L., Hutchison, V. B., Martín, E., Montgomery, E. T., Ladino, C., Tessler, S., and Zolly, L. S., *The United States Geological Survey science data lifecycle model*. US Geological Survey Open-File Report No. 2013–1265, US Geological Survey, 2013, https://doi.org/10.3133/ofr20131265

Government Digital Service (GDS), *Data Sharing Governance Framework* [online], GDS, gov.uk, 2022 ▶

Government Digital Service (GDS), Using metadata to describe data assets in a data catalogue [online], GDS, gov.uk, 2023 ▶

Government Digital Service (GDS), Principles for securing personal data in government services [online], GDS, gov.uk, 2025 ▶

Her Majesty's Government (HMG), *Data maturity assessment for government*, HMG, 2023 ▶

Information Commissioner's Office (ICO), *Guide to the UK General Data Protection Regulation (UK GDPR):* Consent, ICO, 2020 ▶

Information Commissioner's Office (ICO), *Data sharing: A code of practice*, ICO, 2021 ▶

Information Commissioner's Office (ICO), *Right to rectification*, ICO, 2021b ▶

Information Commissioner's Office (ICO), *Data protection impact assessments (DPIAs)*, ICO, 2023 ▶

International Organization for Standardization (ISO), *ISO 9001:2015 Quality management systems – Requirements*, ISO, Geneva, Switzerland, 2015 ▶

International Organization for Standardization (ISO), and International Electrotechnical Commission (IEC), *ISO/IEC TR 10032:2003 Information technology – Reference model of data management*, ISO, Geneva, Switzerland, 2003 ▶

International Organization for Standardization (ISO), and International Electrotechnical Commission (IEC), *ISO/IEC 27001:2022 Information technology – Security techniques – Information security management systems – Requirements* (Annex A: Reference control objectives and controls, ISO, 2022 ▶

International Organization for Standardization (ISO), and International Electrotechnical Commission (IEC), *ISO/IEC 38500:2024 information technology – Governance of IT for the organization*, ISO, 2024 ▶

International Social Security Association (ISSA), *ISSA guidelines: Information and communication technology* (Revised and Extended Edition), ISSA, [member only], 2022 ▶

Kent, K., Mell, P., and Stine, K., *Guide to computer security log management (NIST SP 800-92)*, National Institute of Standards and Technology (NIST), 2006 ▶

Leite, P. G., Karippacheril, T. G., and Lindert, K., *Social registries for social assistance and beyond: A guidance note and assessment tool*, (Social Protection and Labor Discussion Paper No. 1704), World Bank, 2017 ▶

Leite, P., Grosh, M., Wai Poi, M., and Tesliuc, E., *Revisiting targeting in social assistance: A new look at old dilemmas*, Human Development Perspectives, World Bank, 2022 ▶

Lindert, K., Karippacheril, T. G., Rodríguez Caillava, I., and Nishikawa Chávez, K. (eds), *Sourcebook on the foundations of social protection delivery systems*, World Bank, 2020 ▶

National Institutes of Health (NIH), *How to request and access datasets from dbGaP*, NIH, 2023 ▶

National Institute of Standards and Technology (NIST),*Generally accepted principles and practices for securing information technology systems*, NIST Special Publication 800-14, US Department of Commerce, 1996 ▶

National Institute of Standards and Technology (NIST), *Digital identity guidelines: Enrollment and identity proofing (SP 800-63A)*, US Department of Commerce, 2017 ▶

National Institute of Standards and Technology (NIST), *Security and privacy controls for information systems and organizations*, US Department of Commerce, 2020 ▶

National Institute of Standards and Technology (NIST), *The NIST cybersecurity framework (CSF) 2.0*, NIST Cybersecurity White Paper 29, US Department of Commerce, 2024 ▶

Office of Management and Budget (OMB), *Guidance for preparing and submitting security plans of action and milestones (Memorandum M 02 01)*, Executive Office of the President, 2001 ▶

Office of Management and Budget (OMB), *Open data policy: Managing information as an asset (M-13-13)*, OMB, 2013

Office of Management and Budget (OMB), *Delivering a digital-first public experience* (M-23-22), OMB, 2023 ▶

Office for National Statistics, *Office for National Statistics (ONS) data acquisition policy*, ONS, 2023 ▶

Open Data Institute (ODI), ODI Inside Business: Unlocking the power of good data governance [Blog], The Open Data Institute, 2023 ▶

Project Management Institute (PMI), *A guide to the project management body of knowledge* (PMBOK Guide, 7th edition), Project Management Institute, 2021

Sachsse, C., *Real-time monitoring and response plans: Creating procedures*, Abdul Latif Jameel Poverty Action Lab (J-PAL), n.d., ▶

Shah, S. I. H., Peristeras, V., and Magnisalis, I., DaLiF: A data lifecycle framework for data-driven governments, *Journal of Big Data*, 8, 89, 2021 ▶

Swanson, M., and Guttman, B., *Generally accepted principles and practices for securing information technology systems* (NIST Special Publication 800-14), National Institute of Standards and Technology (NIST), 1996, ▶

UNICEF. (2021). *The case for better governance of children's data: A manifesto*. UNICEF Global Insight. ▶

United Nations Economic Commission for Europe (UNECE). *A guide to data integration for official statistics* (Version 2.0). 2024. ▶ US Department of Energy, Service level agreements, US Department of Energy, 2024 ▶

Wagner, B., Ferro, C., and Stein-Kaempfe, J., *Implementation guide: Good practices for ensuring data protection and privacy in social protection systems – A guide for practitioners working and advising in low- and middle-income countries*, Social Protection Inter-Agency Cooperation Board (SPIAC-B), 2022 ▶

World Bank, *Capturing what matters: Essential guidelines for designing household surveys*, World Bank, 2010 ▶

World Bank, *Principles on identification for sustainable development: Toward the digital age*, World Bank, 2017 ▶

World Bank, *Turkey's integrated social assistance system*, World Bank, 2018 ▶

World Bank, Enumerator recruitment and training (DIME Wiki) [online], World Bank, 2022 ▶

World Bank, World development indicators database [online], World Bank, 2025 ▶

Imprint

Published by:
Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Registered offices:
Bonn and Eschborn

Address:
Friedrich-Ebert-Allee 32 + 36
53113 Bonn/Germany
T +49 228 44 60 – 0
F +49 228 44 60 – 17 66
E info@giz.de
I www.giz.de

Dag-Hammerskjöld-Weg 1-5
65760 Eschborn/Germany
T +49 61 96 79 – 0
F +49 61 96 79 – 11 15

Required citation:
Digital Convergence Initiative. 2025. A data governance framework for digital social protection systems. Deutsche Gesellschaft für Internationale Zusammenarbeit, Germany.

Authors
Tim Ohlenburg

Editing
Susan Sellars

Layout / Illustrations:
now [nau], communicative visual design, Frankfurt/Main

Responsible for the content
Ralf Radermacher, GIZ

Bonn, November 2025

Digital Convergence Initiative (DCI)

The DCI receives funding from the European Commission and the German Federal Ministry for Economic Cooperation and Development (BMZ). The secretariat of the DCI is jointly housed at Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ), Expertise France, Foundation for the Internationalization of Public Administrations (FIAP), the International Labour Organization (ILO), and the World Bank.

E-mail: ▶ **contact@spdci.org**
Website: ▶ **www.spdci.org**

Co-funded by

European Union

german cooperation
DEUTSCHE ZUSAMMENARBEIT

Global Gateway

Coordinated by

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

International Labour Organization

THE WORLD BANK

EXPERTISE FRANCE
GROUPE AFD

fiap SISTEMAS PÚBLICOS PARA EL MUNDO