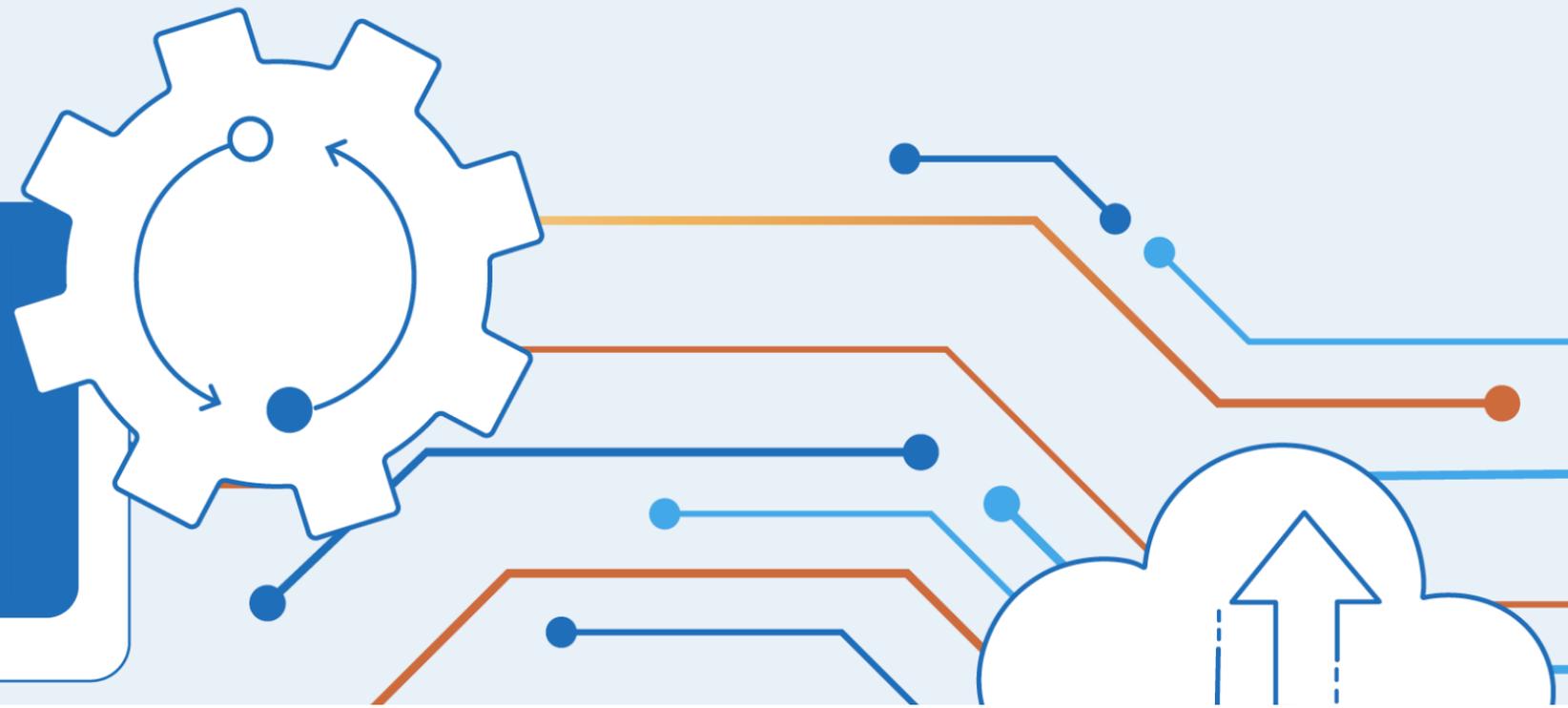# A data governance framework for digital social protection systems

## Launch webinar
February 24, 2026
12:00 - 13:30 GMT

Digital Convergence
USP 2030

Co-funded by:
Global Gateway
European Union
german cooperation
DEUTSCHE ZUSAMMENARBEIT

Coordinated by:
giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH
ILO International Labour Organization
THE WORLD BANK
EXPERTISE FRANCE GROUPE AFD
fiap

# Housekeeping rules

- Ask your questions in the Q&A box

- Share any comments or resources in the chat

To: Everyone ⌄

Your text can be seen by panelists and other attendees

- Simultaneous interpretation is available
Select the language in the interpretation icon on control bar (English, French, Spanish, Portuguese available)

- Session will be recorded

# Agenda

| | |
|---|---|
| 12:00–12:10 | **Welcome and introduction** |
| 12:10–13:00 | **Presentations** |
| 13:00–13:15 | **Discussion** |
| 13:15–13:30 | **Q&A and Closing** |

# About the Digital Convergence Initiative

The **Digital Convergence Initiative (DCI)** is a joint effort by USP2030 to support the **digital transformation of social protection systems**.

Co-funded by:

Coordinated by:

# Our approach

## Knowledge sharing

Open and collaborative **digital knowledge base** on digital social protection

**Knowledge products:**
- ✓ Case studies and reports
- ✓ Guides and toolkits
- ✓ Learning briefs

**Events:**
- ✓ Webinars e.g. Talking interoperability
- ✓ In-person workshops and conferences

## Global technical standards

Global effort to harmonize **technical standards for interoperability**

- ✓ Transparent, multi-stakeholder, consensus-building processes to **develop standards**
- ✓ Open **digital repository** of technical standards
- ✓ Engagement with solutions providers and practitioners to **promote adoption**

## Country implementation support

Digital transformation and interoperability **country support**

- ✓ Direct **implementation** in seventeen selected countries
- ✓ The **Helpdesk** as a technical support facility for expanded outreach to countries to guide on Digital Transformation

## Capacity development & training

Strengthening institutional and human **capacity**

- ✓ Structured **peer learning** opportunities through cross-country exchanges
- ✓ Modular, adaptable and practice-oriented **training programs,** designed for country-specific contexts

Introducing the
Data Governance
Framework

# DCI - Data Governance Framework

**Objectives**
- Map data governance to SP
- Support policy reform
- Give practical guidance

**Target audience**
- Policy makers
- System adminstrators
- SP community

**Caveats**
- Starting point only
- Context, context, context



Digital Convergence
USP2030

A data governance framework for digital social protection systems

Guidance for practitioners, policymakers and system administrators
2025

# Data governance

## Management
**Focus:** Policies and procedures for handling data throughout its lifecycle to ensure operational efficiency and regulatory compliance.

1. **Planning**
Capturing ambitions and responsibilities in a data management plan.
2. **Acquisition**
Directions for primary collection, administrative data exchange, and third-party data.
3. **Processing:**
Converting raw data into operational formats, such as eligibility determination.
4. **Analysis:**
Using metadata and data catalogues to ensure discoverability and risk assessment (e.g. DPIAs).
5. **Sharing and use:**
(Detailed under the Access Pillar).
6. **Archiving and deletion:**
Managing data at the end of its lifecycle through retention schedules and secure disposal.

## Quality
**Focus:** Procedures to ensure data is accurate, consistent, and reliable, enabling better eligibility determination and public satisfaction.

1. **Completeness:**
Ensuring all required individuals and data items are present while following data minimisation.
2. **Accuracy:**
Ensuring records reflect true circumstances via training, pilots, and rectification modalities.
3. **Currency:**
Degree to which data is up-to-date and available when needed.
4. **Consistency:**
Uniformity of data across different records and databases, supported by pre-populated CAPI.
5. **Validity:**
Ensuring data accurately represents the intended measure or concept.
6. **Uniqueness:**
Establishing an unambiguous representation of actors through unique identifiers (UIDs) and master data models.

## Access
**Focus:** Mechanisms ensuring authorised users can retrieve data while maintaining privacy, transparency, and security.

1. **Internal Access:**
Assignment of access rights to staff based on the "need to know" and "least privilege" principles.
2. **External Access:**
Secure data sharing with trusted organisations (e.g. health or education bodies) via formal agreements.
3. **General public (open data):**
Providing anonymised summary statistics or micro-data for research and transparency.
4. **Cross-cutting issues:**
Overarching elements like data access policies, request processes, and consent management.

## Security
**Focus:** Measures to protect data from unauthorised access, accidental destruction, loss, or alteration.

1. **Technical measures:**
Technologies like encryption, multi-factor authentication, and network firewalls.
2. **Organisational measures:**
Governance structures including incident response plans and IT supplier risk management.
3. **Physical measures:**
Restricting physical access to facilities and ensuring hardware protection and backups.
4. **People:**
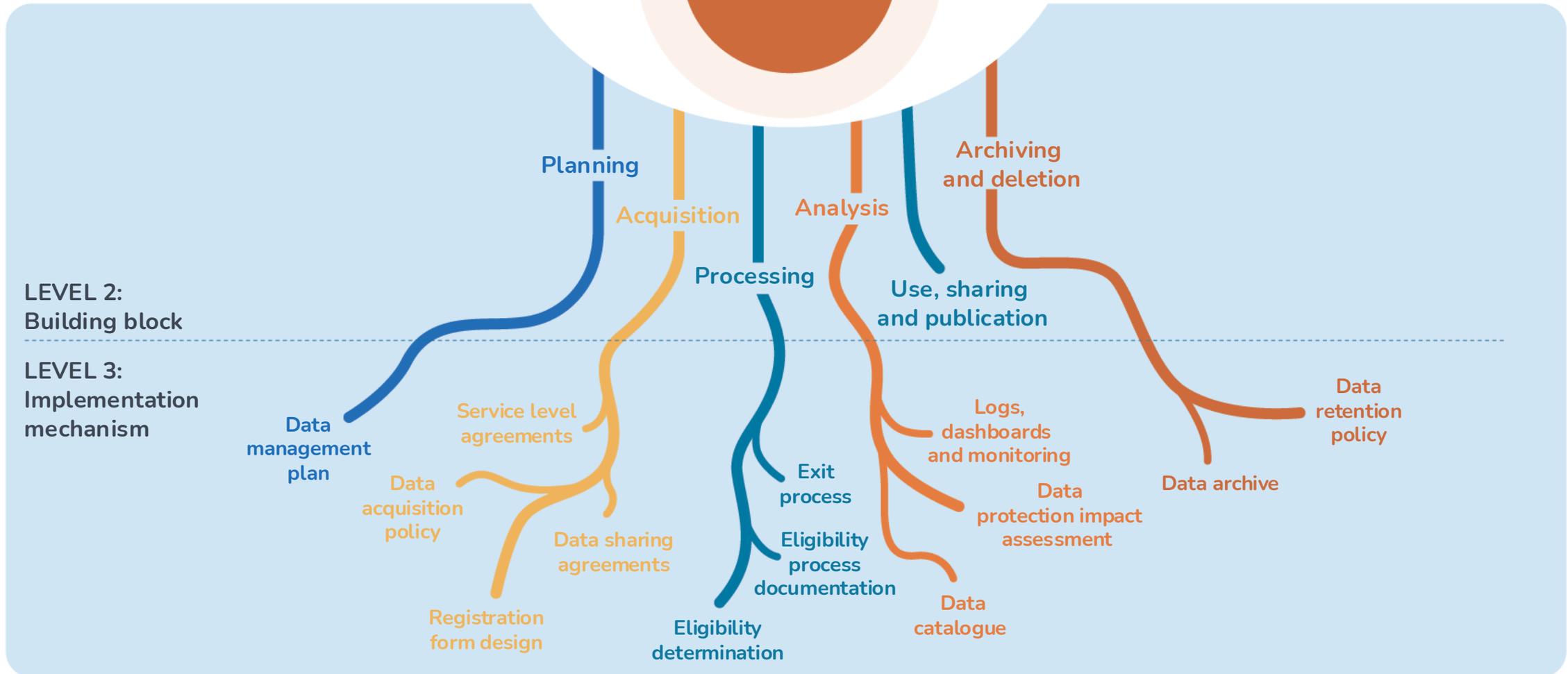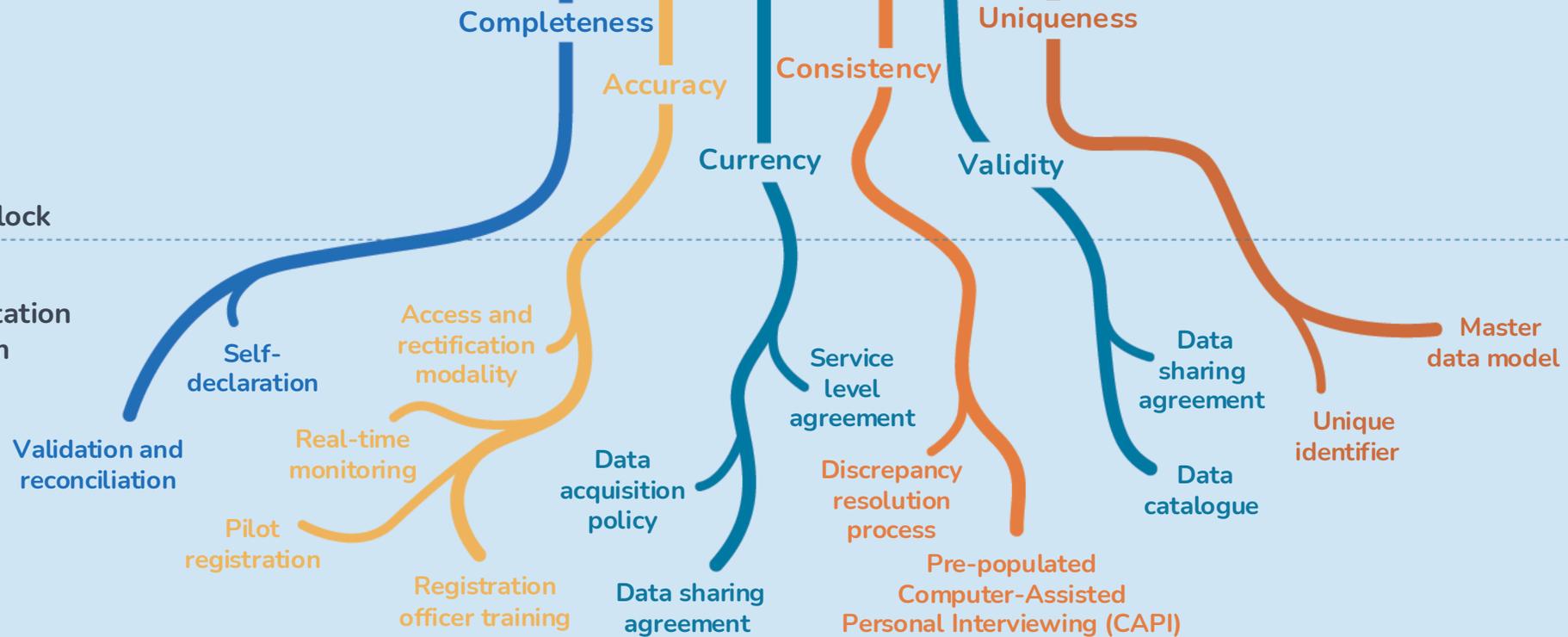Fostering a security-conscious culture through staff training and insider threat management.

Pillar 1

Management

Focus:
Policies and procedures for handling data throughout its lifecycle to ensure operational efficiency and regulatory compliance.

LEVEL 2: Building block

LEVEL 3: Implementation mechanism

Planning

Acquisition

Analysis

Archiving and deletion

Processing

Use, sharing and publication

Data management plan

Service level agreements

Data acquisition policy

Data sharing agreements

Registration form design

Exit process

Eligibility process documentation

Eligibility determination

Logs, dashboards and monitoring

Data protection impact assessment
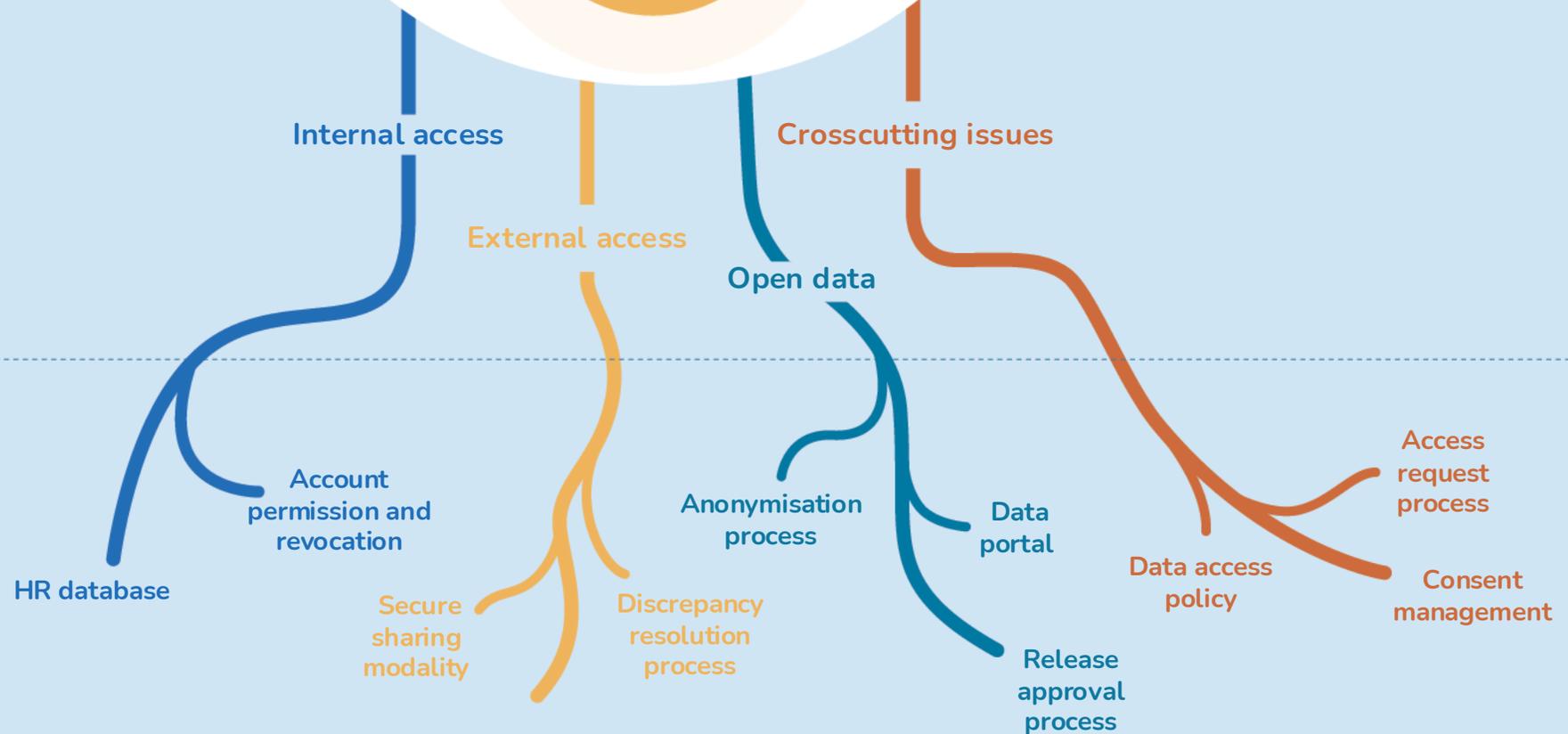
Data catalogue

Data archive

Data retention policy

Pillar 3

Access

Focus:
Mechanisms ensuring authorised users can retrieve data while maintaining privacy, transparency, and security.

Internal access

External access

Open data

Crosscutting issues

LEVEL 2:
Building block

LEVEL 3:
Implementation mechanism

Account permission and revocation

HR database

Secure sharing modality

Discrepancy resolution process

Anonymisation process

Data portal

Release approval process

Data access policy

Access request process

Consent management

# Pillar 4



Security

Focus:
Measures to protect data from unauthorised access, accidental destruction, loss, or alteration.

**Technical**

**Organisational**

**People**

**Physical**

LEVEL 2:
Building block

LEVEL 3:
Implementation mechanism

Encryption

Penetration testing

Authentication

Patches and updates

Data loss prevention

Endpoint security

Network security

Regular security review

Incident response plans, disaster recovery and business continuity

IT supplier risk management

Secured access

Backup and recovery

Device protection

Insider threat management

Training

# Implementation cycle(s)

## Steps

1. **Convene** — Secretariat + stakeholders
2. **Scope** — Prune + extend
3. **Profile** — Status quo + gaps
4. **Plan** — Prioritization + project plan
5. **Implement** — 12-18 month cycle

(... repeat)
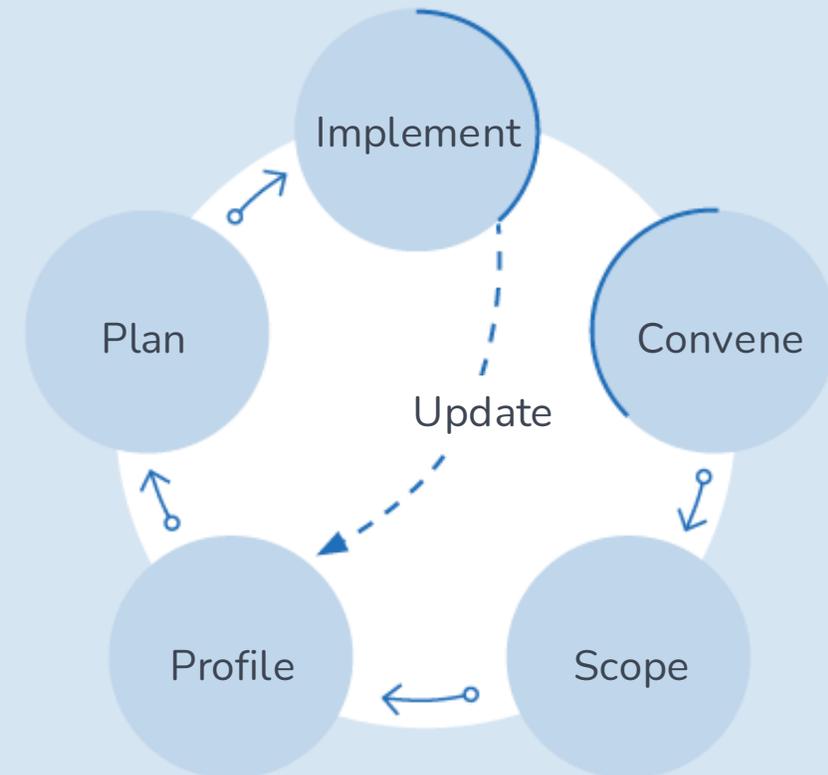
Verónica Achá Alvarez
Head of the Social Information Division
Ministry of Social Development and
Family
February 24th, 2026

# Chile's approach to data governance and the 'Only ask once' policy

# The 'Only ask once' policy

People, in their dealings with the Administration, have the right:

d) To be exempt from submitting documents that <u>do not correspond to the procedure</u> or <u>that originate from</u> and <u>are in the possession of any body of the State Administration</u>. In the latter case, said documents must be sent by the body that has them in its possession to the one that is processing the administrative procedure;

# How do we make
# the 'Only ask once' statement
# a reality?

# The story of Inés



*This is Inés, a 45-year-old woman who lives with her mother and her 7-year-old son.*

*She is currently in the 50% vulnerability bracket of the Social Registry of Households.*

*She has a small business with low sales, which she used to supplement her formal employment.*

*But Inés lost her main job and feels overwhelmed. She must be able to support her household.*

**Inés needs to navigate the social protection system to find out if there is support or assistance available for her and her family.**

# Chile has a broad... but (maybe) complex social protection system



Number of programs by type of beneficiary
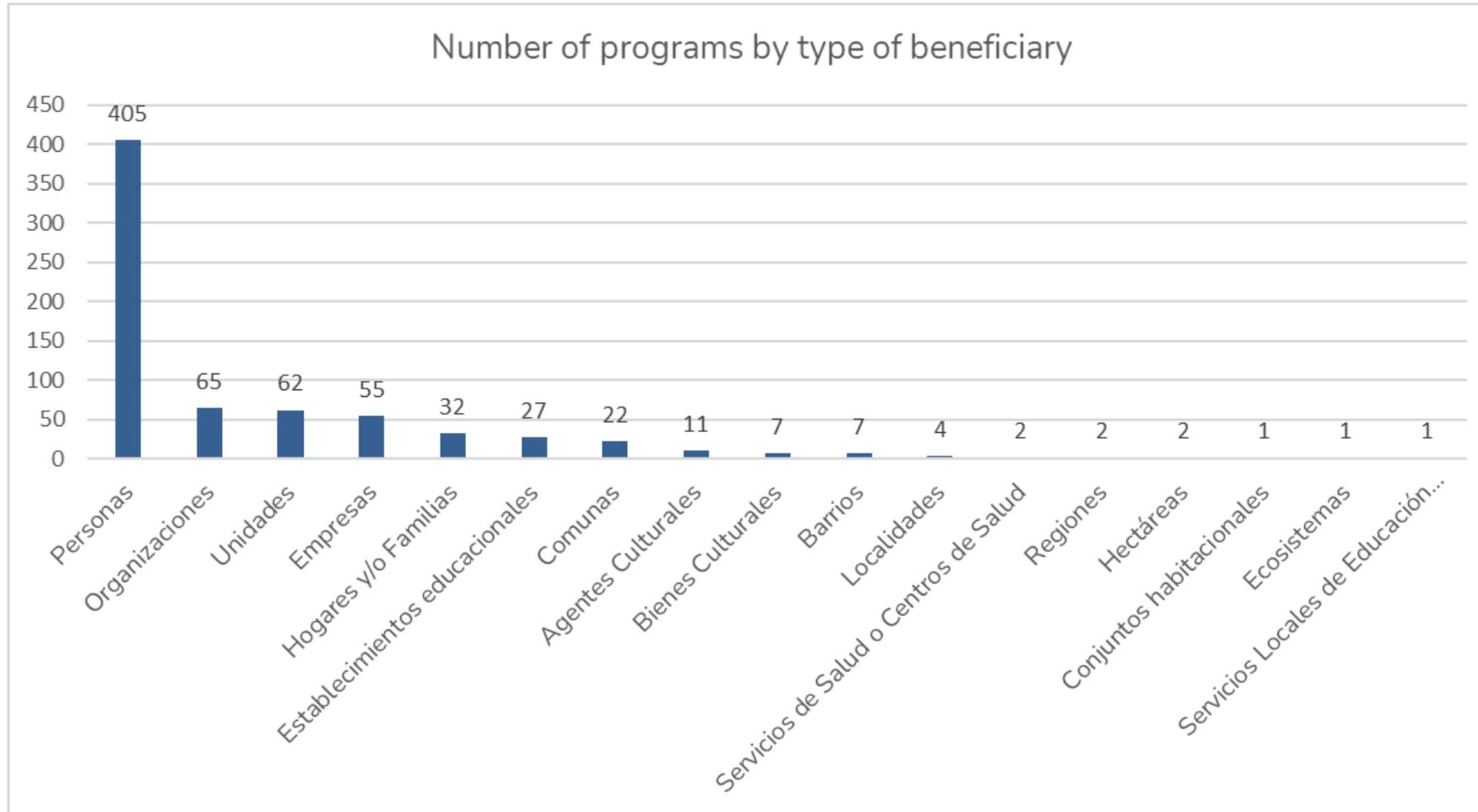
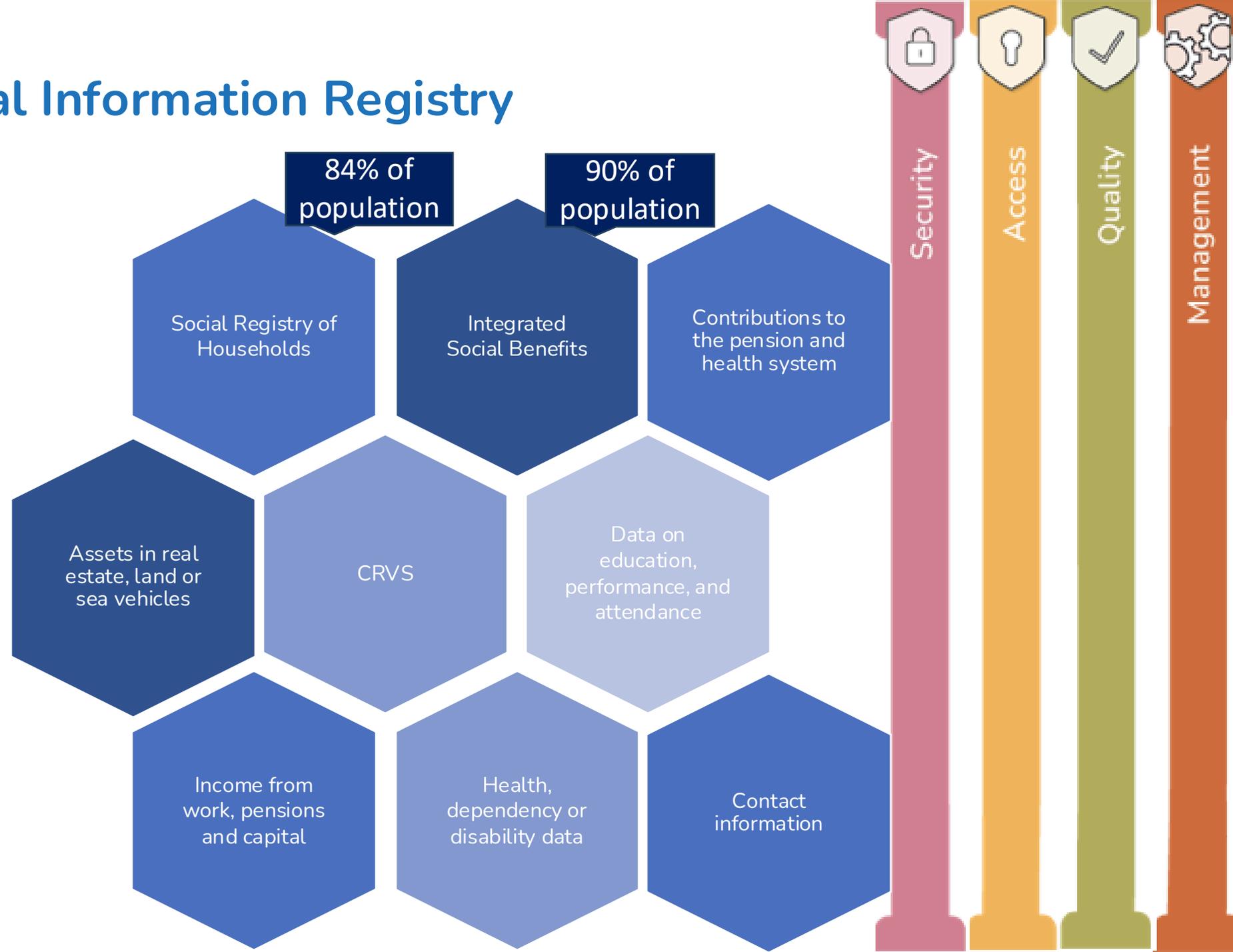*In 2024, the Chilean government funded 706 public programs, both social and non-social:*

*- 405 were directed at individuals*

*- 301 were allocated to other types of users*

# The Social Information Registry

- RIS was created by law in 2004 and is administered by the MDSF.

- The data is connected through the unique national ID number (RUN).

- RIS interoperates with several public institutions; we have signed detailed agreements.

- Data governance is in place, and a cybersecurity system too.

**84% of population**

**90% of population**

- Social Registry of Households
- Integrated Social Benefits
- Contributions to the pension and health system
- Assets in real estate, land or sea vehicles
- CRVS
- Data on education, performance, and attendance
- Income from work, pensions and capital
- Health, dependency or disability data
- Contact information

Security

Access

Quality

Management

# The State's Digital Transformation Law

*A Law to be implemented **progressively** between 2022 and 2027.*

*To promote that the complete cycle of administrative procedures, for all State Administration bodies subject to the Law on the Bases of Administrative Procedure (19.880), must be carried out electronically.*

*To provide greater **certainty**, **security**, and **speed** in the delivery of services to the public, along with greater transparency in the State's processes and actions in its relationship with citizens.*

*The administrative bodies are required **to provide and properly use** electronic platforms for the purpose of **maintaining electronic records**, which must comply **with standards of security**, **interoperability**, **interconnection** and **cybersecurity**.*

# Key aspects of the State's Digital Transformation Law

| Digital Communications | Digital Notifications | Administrative Procedures | Electronic Files | Document Digitization | Interoperability |

This is how we shall help Inés
finding out if there is support
or assistance available
for her and her family:

**The one stop shop for social benefits**

# Ventanilla Única Social:
# one stop shop for social benefits

- Login secured using the personal digital ID provided by the Civil Registry: "Clave Única".

- More than 130 procedures, benefits, and social services from various institutions were integrated into a single platform.

- We can help identify eligibility for over 100 benefits using administrative records available at the Ministry, including the Social Register of Households, thus easing the bureaucratic burden on individuals.

Pillar 3. Access

Pillar 4. Security

You are logged in

Social Registry of Households vulnerability bracket

Main menu

Notifications

# Türkiye's approach to data governanceand the dynamic data

Ercan Dansuk - Ministry of Family and Social Service – Türkiye

Senior social Protection Specialist

# Türkiye's Approach to Data Governance for SP

**Integrated Social Assistance Information System (ISAS):**

**a software program that enabled the collection of supporting documentation for the social assistance application to be completed automatically online.**

- A comprehensive data governance framework supporting **efficient, fair, and responsive social protection**

- Built on **interoperable administrative data**, local verification, and strong safeguards

- Aligned with PDPL, public administration standards, and international best practice

# 1. Management

**Data management** plan covers digitisation of social assistance processes, purpose of data collection, signed protocols that include defining roles and responsibilties of institutions and data dictionary.

**Processing** data has converting raw data into operational formats (standardised, validated, and usable formats).

**Sharing Use process** ensures that data is used only for clearly defined and authorised purposes throughout the system.

**Acqusition** includes primary data collection (administrative data, household visits, self-declaration), administrative data Exchange (social registry)

**Analysis** focuses on structured use of data for monitoring, evaluation, and policy design by creating metadata standards and data catalogues and includes Data Protection Impact Assessments (DPIAs).

**Archiving and Deletion** cover managing data at the end of its lifecycle through retention schedules and secure disposal ISAS manages the end of the data lifecycle through defined retention periods aligned with legal, operational, and audit requirements.
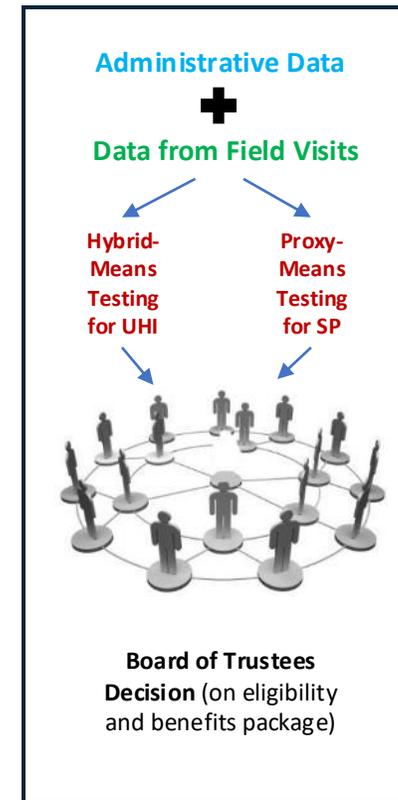
# Processes in ISAS



| Assess | Enroll | Provide/Monitor |

**Assess**

**Administrative Data**

Cadastral · Social Sec. · Housing · Tax · Banking · Health · Employment · Education · Civil Reg · Assets · Address

**Data from Field Visits**

HH visit

**Streamlined flow of information** between agencies and programs to create and update beneficiary profiles (real-time data collection from administrative sources)

**HH visits** (data collection by physical interaction)

**Linked with 24 Public Entities with over 120+ webservices**

**HH visits by ~5,000 social asst. workers in 1,000 SASFs**

**Enroll**

**Administrative Data**
**+**
**Data from Field Visits**

Hybrid-Means Testing for UHI

Proxy-Means Testing for SP

**Board of Trustees Decision** (on eligibility and benefits package)

**"Dynamic & Integrated" gateway for multiple (50+) SP programs**

**Provide/Monitor**

Auditing · Data Analytics · Beneficiary Monitoring

Payments — Ptt

**Provision of Services & Benefits** (payments, service delivery, beneficiary monitoring, auditing, reporting, etc.)
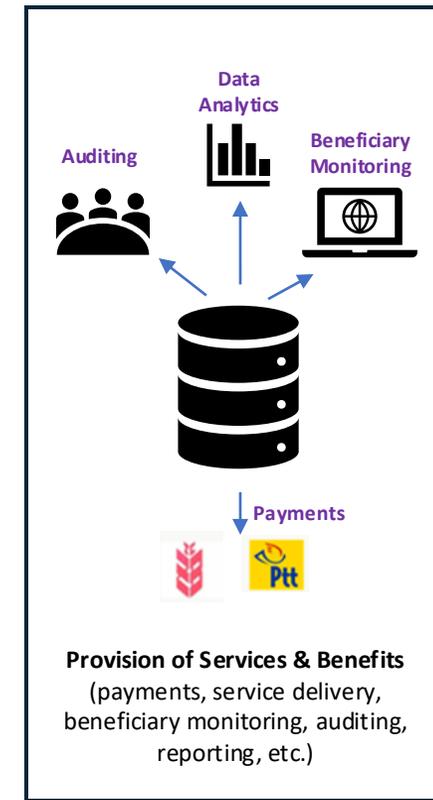
**Covers 15+ million households and 60+ million individuals.**

# 2. Quality

**Completeness** is achieved by defining **standardised minimum datasets** required for eligibility assessment, case management, and benefit delivery. Household applications are structured to ensure that all relevant individuals (household members, dependants) and essential socio-economic variables are captured.

**Accuracy** ensures records reflect true circumstances through training, pilots, and rectification mechanisms. It is supported through a combination of **human, procedural, and system-based controls**. Frontline staff and social workers receive regular training on data collection standards, interview techniques, and verification practices in ISAS.

**Currency** is that ISAS addresses this by combining interoperable administrative data with regular household-level updates conducted by local social assistance foundations.

**Consistency** Ensures uniformity across records and databases, supported by pre-populated CAPI. Consistency in ISAS is achieved by using common definitions, coding standards, and reference data across institutions. Pre-populated Computer-Assisted Personal Interviewing (CAPI) tools reduce manual entry and ensure that data collected in the field aligns with existing administrative records.

**Validity** in ISAS refers to whether collected data truly measures the socio-economic concepts it is intended to represent (e.g. vulnerability, dependency, or need). This is addressed through carefully designed indicators, alignment with social policy objectives, and periodic reviews of eligibility criteria.

**Uniqueness** ISAS ensures uniqueness by relying on national unique identifiers (UIDs) and master data management principles. Each individual and household is represented once, preventing duplication across records and programmes.

# PROCEDURES OF GATHERING INFORMATION & DATA: APPLICATION PHASE

Application with only
**national identity number**
**via "e-Government Gateway"** (online)
**or to the 1003 SASFs** (personally)

The application standardizes declaration-based data

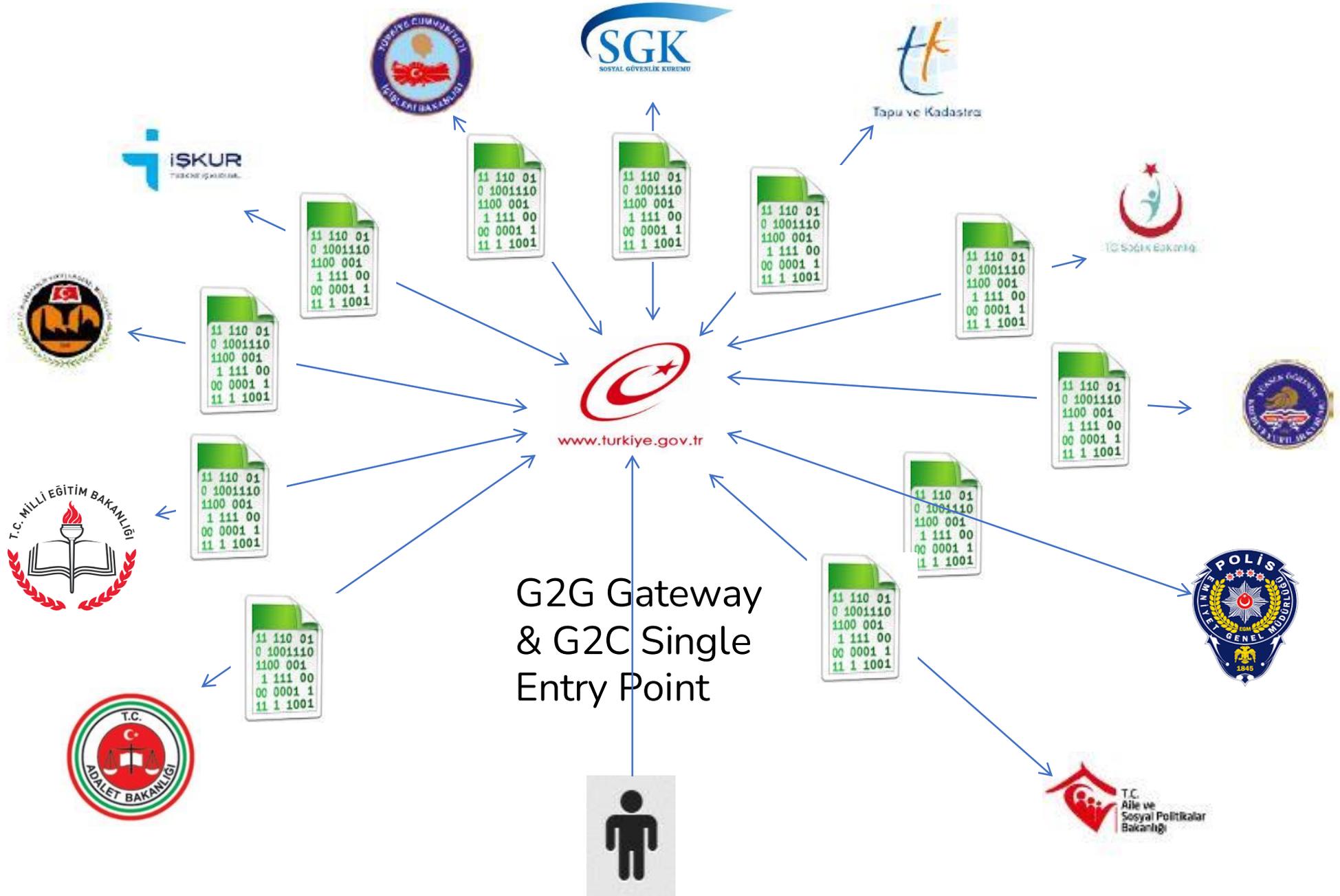Easily integrated with different databases and verified

Submit a signed consent form to allow institutions to review their information

**Application:** applicant's household, employment information, household composition, property ownership etc...

# Administrative Data



G2G Gateway
& G2C Single
Entry Point

www.turkiye.gov.tr

# *Deep dive: Dynamic Data*

Dynamic data in ISAS refers to a shift from **static, infrequently updated data sources**—such as large-scale household surveys and fixed proxy means tests—towards a **continuously updated, interoperable, and field-verified data ecosystem**.

ISAS addresses these challenges by integrating **multiple administrative data sources**

Data-sharing arrangements and technical interfaces allow information to flow automatically into ISAS from relevant registries and databases.

The dynamic updating capability of ISAS allows social assistance programmes to **adjust eligibility and benefit levels more frequently and more fairly,** supporting both routine operations and crisis response.

Regular household visits allow staff to: verify information obtained from administrative sources, register newly vulnerable households, and capture qualitative changes in living conditions that administrative data alone cannot detect.

In combination with strong data governance across **management, quality, access, and security**, dynamic data allows ISAS to move beyond static welfare administration toward **modern, evidence-driven social assistance delivery**.

# 3. Access

Access concerns the policies, institutional arrangements, and technical mechanisms that ensure authorised users can access and use data efficiently, while fully respecting privacy, transparency, data protection, and security requirements.

**External Access** secure data sharing with trusted organisations through formal agreements
ISAS enables external access through structured and legally grounded data-sharing arrangements with trusted public institutions, such as health, education, employment, or social security bodies. These exchanges are governed by formal protocols or agreements that define the purpose, scope, frequency, and safeguards of data sharing.

**Internal Access** covers Role-based access aligned with "need to know" and "least privilege" principles. Internal access in ISAS is governed through **role-based access control (RBAC)** frameworks.

**General Public Access** provides anonymised data for transparency, research, and accountability. ISAS supports transparency by enabling the publication of aggregated or anonymised data products, such as summary statistics on beneficiaries, coverage, and expenditure.

# 4. Security

**Security** addresses the technical, organisational, physical, and human measures implemented to protect ISAS data from unauthorised access, accidental or unlawful destruction, loss, alteration, or disclosure.
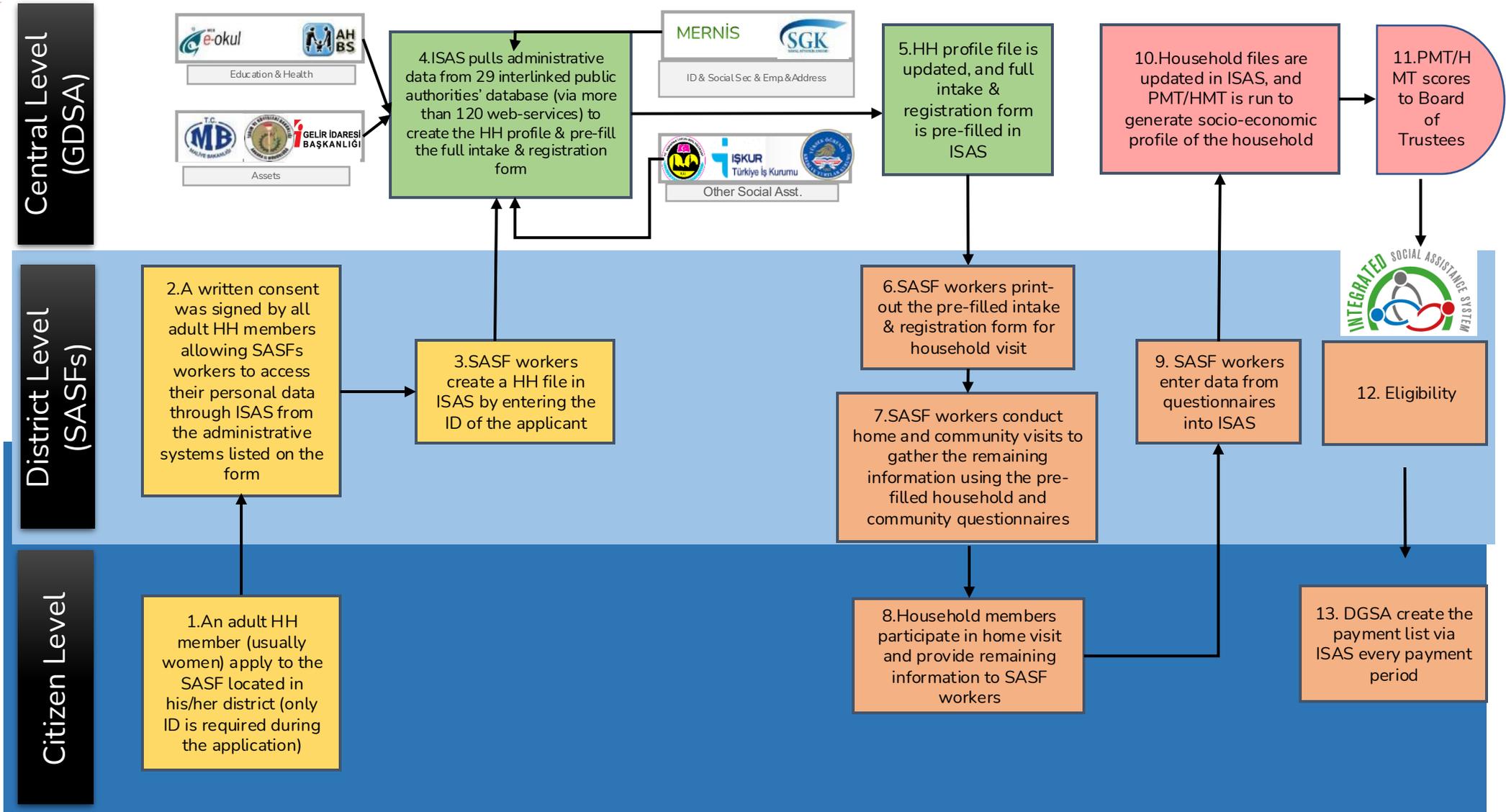
**Technical Measures:** ISAS applies a range of **technical safeguards** to protect data at rest and in transit. These include encryption, secure authentication mechanisms such as multi-factor authentication, and network protections such as firewalls and intrusion detection systems. Access to the system is logged and monitored, allowing suspicious activity to be detected and investigated.

**Organisational Measures:** ISAS relies on organisational security measures that define responsibilities, escalation procedures, and oversight. These include formal incident response plans that specify how security breaches are identified, reported, contained, and remedied.

**Physical Measures:** Physical security in ISAS focuses on controlling access to data centres, server rooms, and office environments where sensitive data or equipment is located. Access is restricted to authorised personnel, and critical infrastructure is protected against theft, damage, or environmental risks.

# Processes in Türkiye's ISAS

Discussion & Q&A

# Learn more about Data Governance, discover our publication



Nov 28, 2025 · Digital transformation

## A data governance framework for digital social protection systems

LEARN MORE →

## Share your thoughts

Enjoyed this piece? We would love to know what you think. Your feedback helps us make our work better.

PUBLICATIONS SURVEY →

# Support the Initiative

## Your input matters

- **Contribute your expertise** to our workstreams

- **Support** the  process of **consensus building and harmonization of standards**

- **Spread awareness** about the initiative

- **Adopt the standards and other outputs** in your projects and share **feedback**
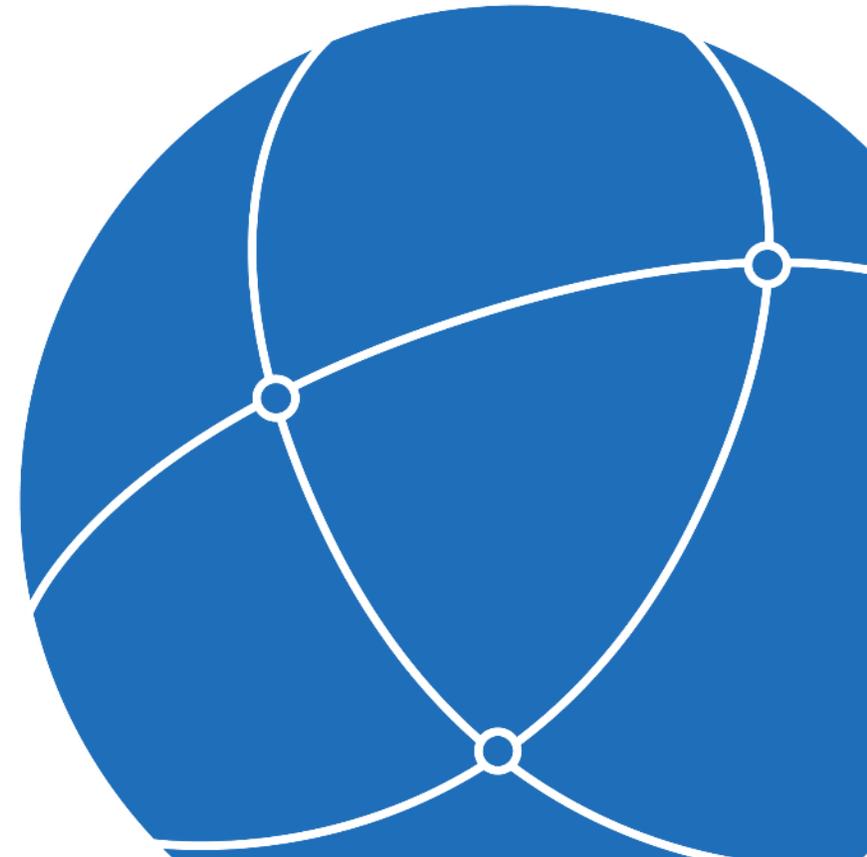
## Forms of participation

- **Share** existing **materials**

- **Review** outputs

- **Join** group **discussions** and workshops

- **Submit your draft standards** to DCI for consensus building through DCI standards committees

- **Join the standards committees**

# Learn more and connect

The DCI is an **open, transparent and virtual community** which welcomes contributions from diverse stakeholders.

For more information, or to get involved:

✓ visit our **website**

✓ email us at **contact@spdci.org**

✓ or check us out on **LinkedIn**, **Gitbook,** and **Github**

Thank you