

Safeguarding data confidentiality in Banca d'Italia: current practices and future challenges

Workshop on Data security and privacy
Lisbon, Portugal, 14-15 September 2026

Many concepts, one governance challenge

CONCEPT	SCOPE	REGULATIONS
Personal Data	Identifiable natural persons	GDPR
Confidential Statistical Information	Identifiable natural and legal persons (including reporting agents)	ECB statistical framework Council Regulation (EC) No 2533/98
Bol Individual Data	Identifiable natural and legal persons (excluding reporting agents)	Bol internal confidentiality framework

The challenge is not defining confidentiality.
The challenge is governing it consistently across increasingly integrated data ecosystems.

Confidentiality management extends beyond privacy compliance and requires integrated governance, accountability and access controls.

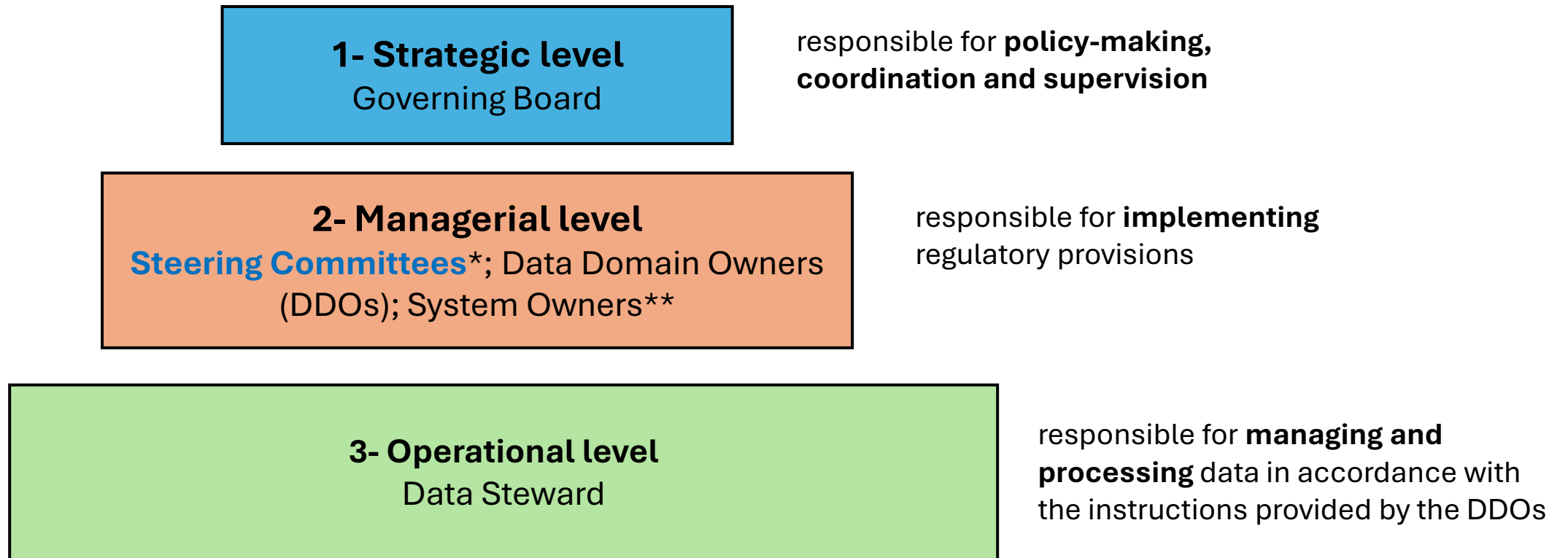
Data governance and technology: two sides of the same coin



Confidentiality protection is effective only when **governance and **technology** are designed together.**

GOVERNANCE + TECHNOLOGY = TRUSTED DATA

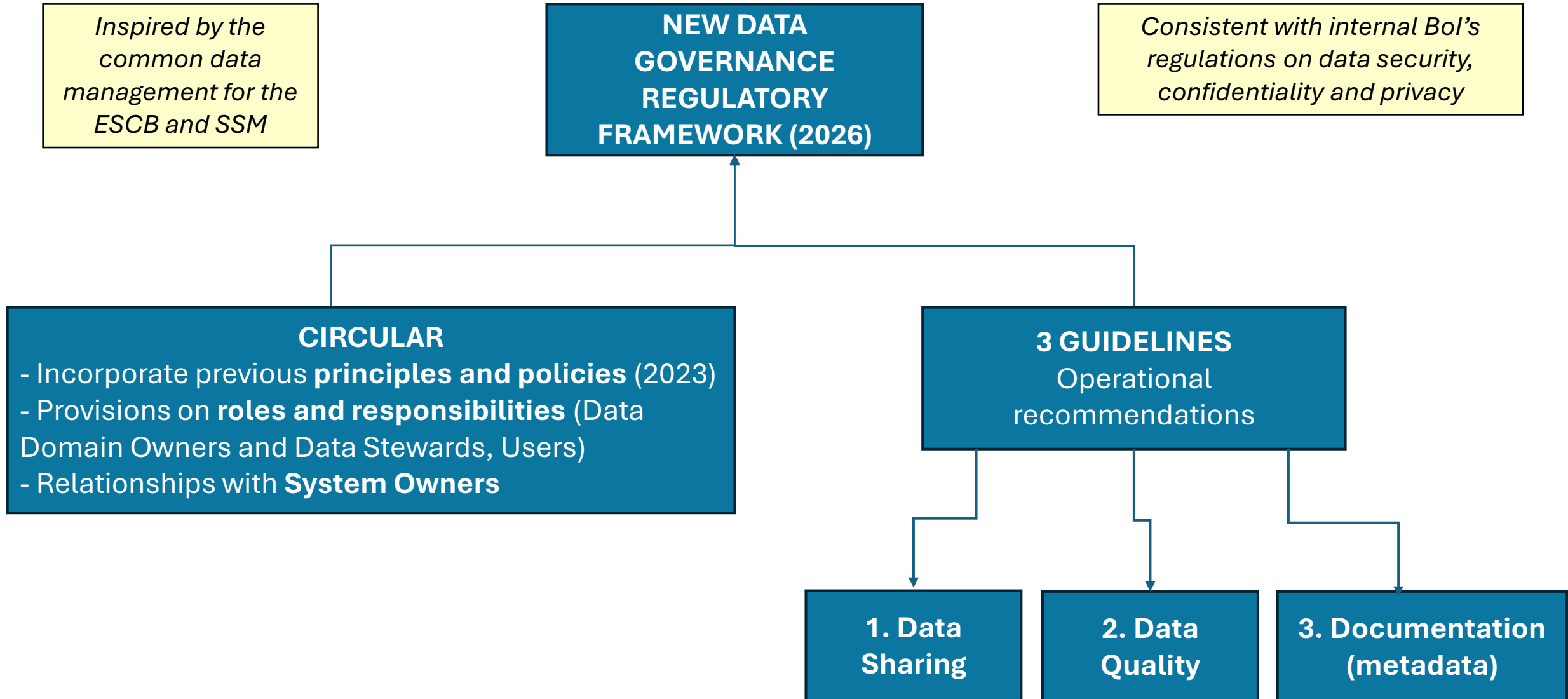
A three-layer Data Governance organizational structure in Bol



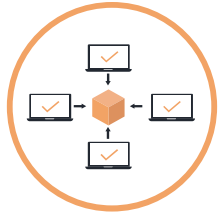
* The **Statistics Committee and Corporate Information Management Committee** act as a liaison in the management of the respective information assets and in resolving any disputes regarding access to data.

** the System Owner is responsible for the IT assets used for the storage, processing and utilization of data.

Recent developments in Bol's Data Governance Framework



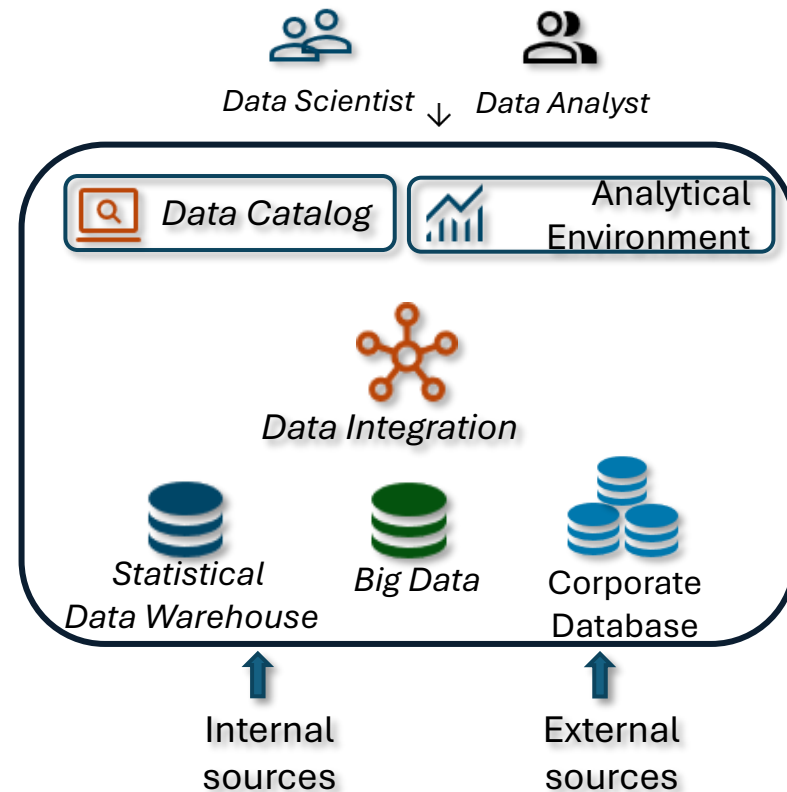
Main objectives of the Enterprise Data Lake (EDL)



Integration
of different data
sources



New analytical and visualization
(also self-service) **tools**



Catalog as a unified point
of access and discovery



**Collaboration and
sharing** environment



Data Governance support

EDL – available tools and capabilities

The same governed ecosystem, with access shaped by **user profile**

FOR ALL ANALYSTS

Data analysts + data scientists



Hue

Explore files and tables

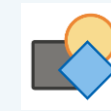
SQL • data analysis



Power BI

Build no-code reports

Dashboards • analysis



Data Catalog

Discover and govern data

Metadata • stewardship

FOR DATA SCIENTISTS

Specialist tools for programming and data engineering



Shiny

Programmatic dashboards

R • Shiny



Notebook

Advanced analyses

R • Python • Julia



Spark

Large-scale analytics

Python • R



Git

Collaborative code

Version control



ETL engine

Build data pipelines

Data engineering



Data Virtualization

Create virtual data views

Data modelling

The Data Catalog of the EDL

Minimum set of common metadata managed by Data Stewards:

- **Mandatory** (e.g. id code, description, frequency, topics)
- **Optional** (e.g. additional documentation)

Two levels of data classification:

1. **Database** (less granular)
2. **Data assets** (single table/file, more granular)

-
- **Data classification: levels of confidentiality, availability and integrity risks**
 - **Accountability: Data Domain Owner and Data Steward**
 - **Possible restrictions:** limits to circularity and data access

(Business) Data Stewards are experts of the data domain, accountable for the metadata management and the data protection according to the rules defined by respective Data Domain Owners.

They can **assign additional metadata** to single table/columns **to apply data protection rules** based on users' need: **masking, hashing, etc...**

The Data Catalog increases users awareness on data classification and governance!

Main measures applied in Bol to guarantee data confidentiality

A distinction between technical and organizational safeguards, with a common objective: reducing risk throughout the data lifecycle.



IT SAFEGUARDS

Technical measures

- **Encryption** at rest and in transit of all data
- **Malware scanning** on ingested data
- **Auditing of all users' activities** and **logging of unencrypted identification codes of extracted individual data** (incl. o/w Politically Exposed Persons)
- Periodic (and historical since ever) **exchange of encrypted subject codes** at least once a year (natural and legal persons)
- Possibility to **mask** with random values, use **hash/encryption functions**, **remove** specific values (based on complex conditions) for individual attributes
- **Availability of different and more flexible tools** (e.g. access to external systems, installation of additional software package) to use less confidential data.



GOVERNANCE SAFEGUARDS

Organizational measures

- **Leading principles:** need to know, least privilege, maximization of usefulness, minimum time of access
- **Formal requests** to access data must be sent by functional email of the business units
- **Authorization check** in case of transfers between business units.
- Internal users must explicitly **sign and comply with the Ethical Code of the Statistician, the ESCB Public Commitment on European Statistics** and, if using individual data, **the attendance of a data privacy course**.
- **Weekly reports** are provided to senior managers containing existing authorizations (**ex ante check**) to allow them to verify the appropriateness of the visualization of individual data by their staff (**ex post check**).
- **Retention policies**

Trusted data comes at a cost: protection vs accessibility



Practical strategies to balance protection and analytical needs

RISK-BASED APPROACH

Adapt protection to the confidentiality level of the data and the actual business need.

TIERED ENVIRONMENTS

Offer multiple platforms with differentiated protection levels (e.g. IT platforms other than EDL).

STANDARDIZED TOOLS

Provide approved tools and libraries while preserving analytical capabilities.

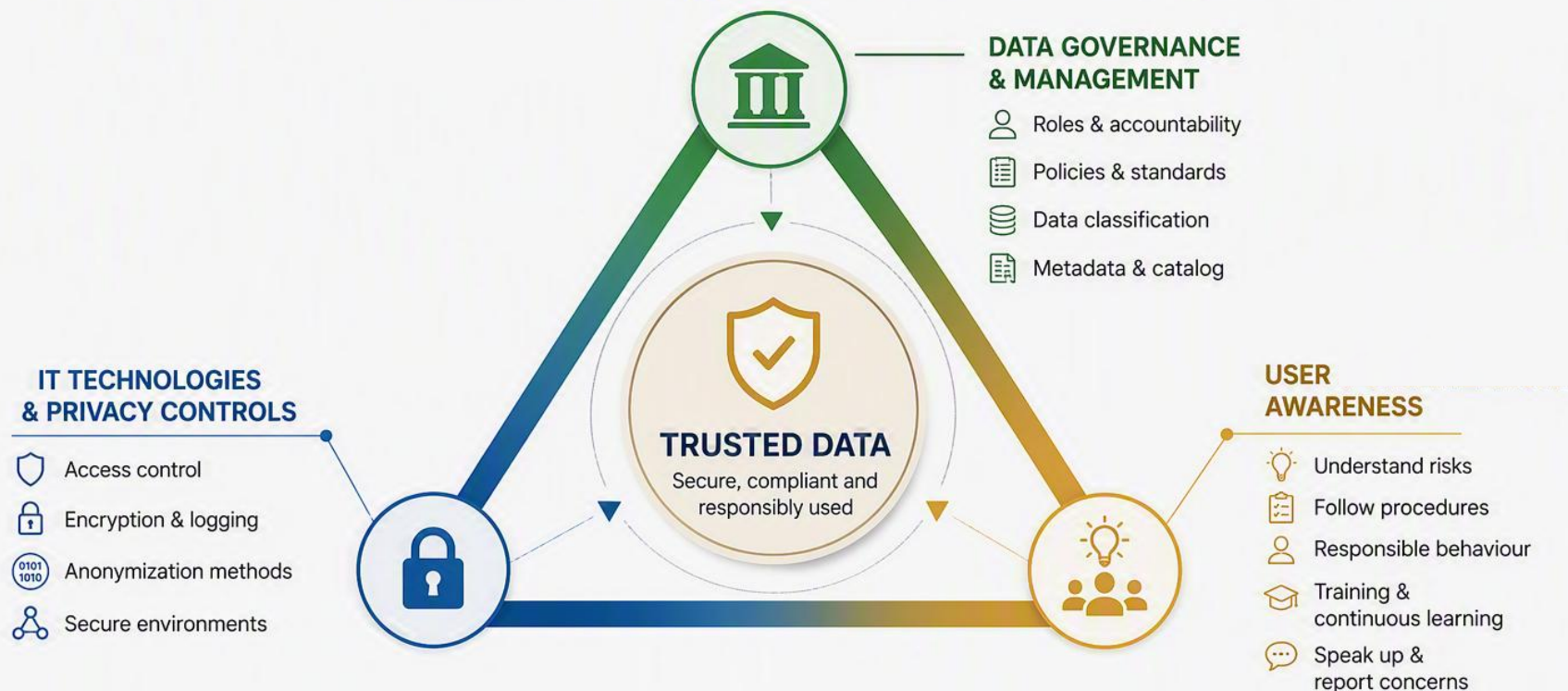
STREAMLINED PROCESSES

Reduce unnecessary burden without weakening controls.

Users awareness: the third pillar

THREE DIMENSIONS OF TRUSTED DATA

Governance, technology and awareness must evolve together



IF ONE DIMENSION LAGS BEHIND, RISKS INCREASE



Data breaches



Re-identification risk



Compliance failures



Misuse of data



Loss of trust



GOVERNANCE defines the rules. | **TECHNOLOGY** enforces the controls. | **AWARENESS** makes them work in practice.

TOGETHER WE ENABLE TRUSTED, RESPONSIBLE AND EFFECTIVE DATA USE.



Thank you for your attention!

Contact Email:

Emiliano.Svezia@bancaditalia.it

Any questions?