

Workshop on data security and privacy

Banco de Portugal and Irving Fisher Committee

14 and 15 September 2026, Lisbon

More Data, **Less Trust?**

The Data-Trust Paradox: Enabling Innovation Without Losing Public Confidence



OPENING KEYNOTE

Dr. Yasser Al Helaly

Cybersecurity Professor | Universidade Nova de Lisboa |
NOVA Information Management School

OPENING ROADMAP

How this keynote **unfolds**

Starting from the workshop's own contributions and moving toward the central paradox.



Research submissions → Clusters → Five workshop sessions



The clusters provide the intellectual foundations of the workshop.

Workshop on data security and privacy

Banco de Portugal and Irving Fisher Committee

14 and 15 September 2026, Lisbon

Trust Is the New **Constraint on Innovation**

In financial services, data value scales only when trust keeps up.



5.7×

more likely to trust a brand
when customers feel
emotionally connected



36%

industry outperformance
for companies excelling at
emotional engagement

“

*“Privacy has shifted from policy
to operational reality.”*



Data privacy is becoming
the constraint on banking
innovation.

Source: Forbes articles, 2026.

What are we collectively **talking about?**

23 contributions. Multiple institutions. One interconnected problem space.

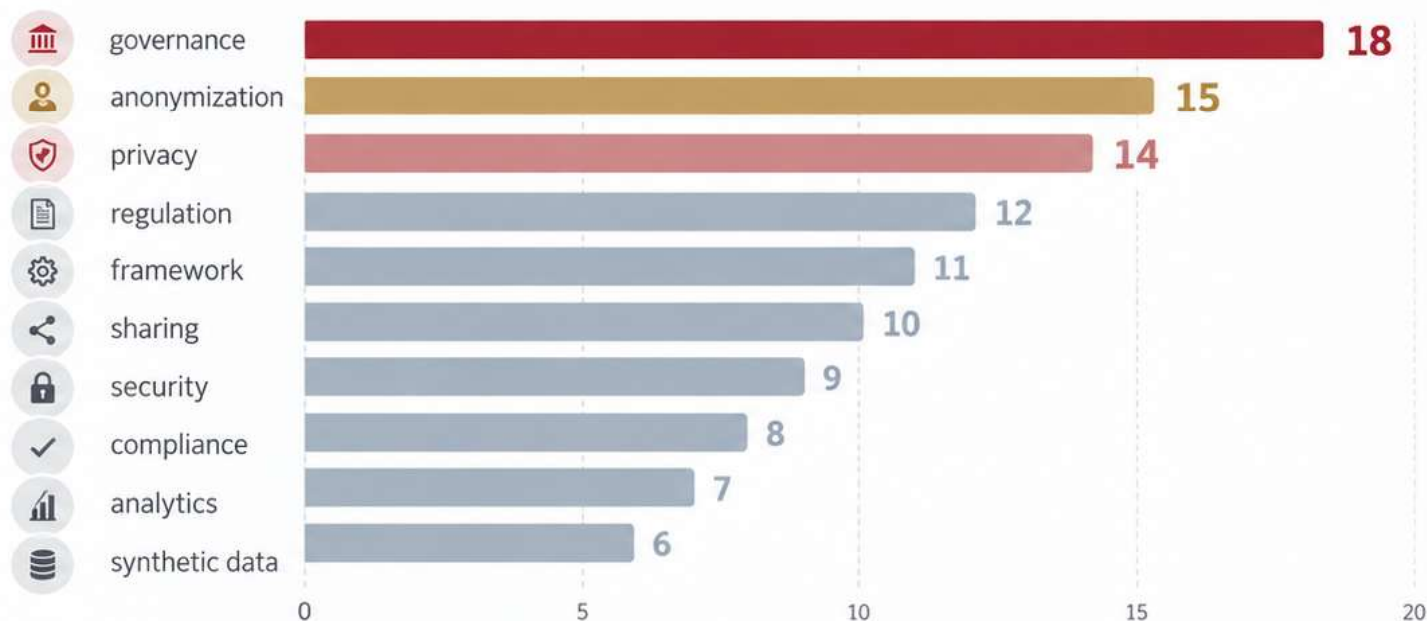
Thematic map of workshop contributions
Based on thematic analysis of submitted abstracts.



This is not a collection of isolated privacy problems. It is **an interconnected data-governance ecosystem.**

Where is the research **attention concentrated?**

Main research hotspots across submitted abstracts and summaries.



Extracted from submitted abstracts and summaries.



Governance leads the agenda.

With 18 mentions, governance attracts the most research attention, ahead of anonymization (15) and privacy (14).

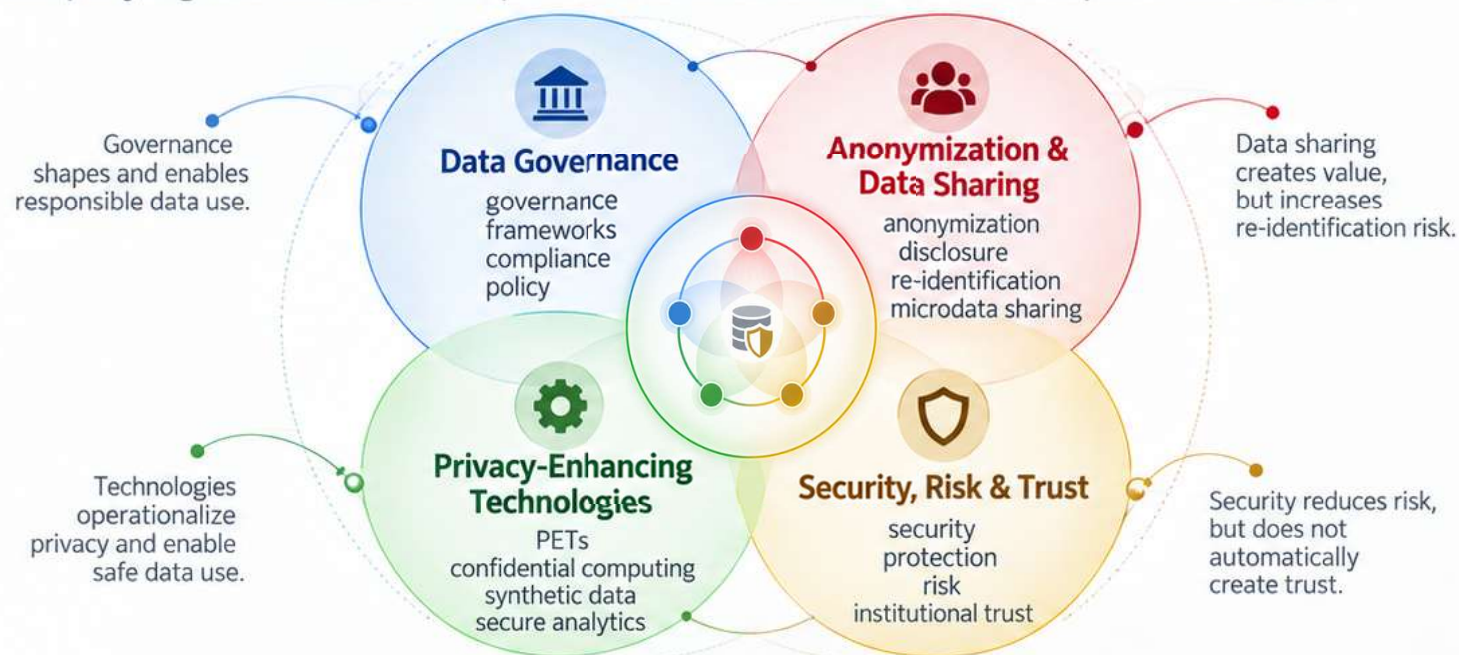


The strongest signal is governance, not technology.

The focus is on institutional, regulatory and trust-related dimensions, highlighting that data governance is central to the debate.

Four clusters emerge

Simplifying the thematic map into four interconnected conceptual domains.



Why interconnected?



Anonymization spans governance, technology, and risk.



Synthetic data belongs to both technology and governance.



Security does not automatically generate trust.



These clusters are analytically distinct, but **operationally interconnected**.

From four clusters to **five workshop sessions**

A visual bridge from the research landscape to the workshop agenda.

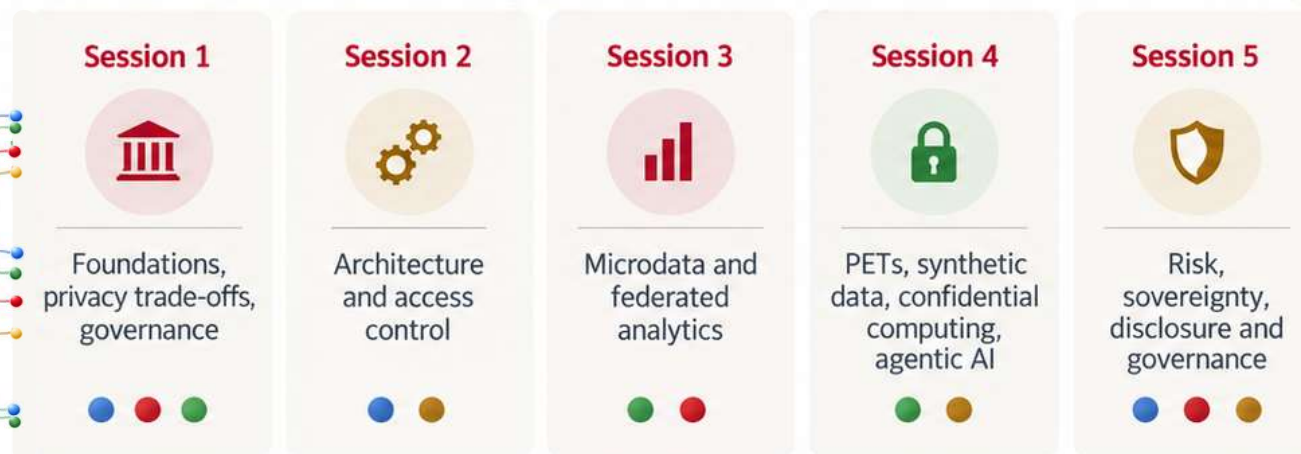
Research clusters

(from submitted abstracts)



Workshop sessions

(from research themes to discussion agenda)



The clusters describe the problem space. **The five sessions describe how this workshop will explore that space.**

One question sits underneath all five sessions

How much **value** can we extract from data without consuming the **trust** that makes its use legitimate?



Why this problem has become **urgent**

Four forces are reshaping the governance challenge.

Open finance ecosystems

Expanding data flows beyond traditional banking, with more actors and new business models.



CBDCs and digital identity

New forms of digital money and identity increase data granularity and linkages across domains.



Interconnected data ecosystem

More data. More actors.
Greater interdependence.



Cross-institutional data sharing

Growing collaboration across public and private sectors increases value, but also complexity and re-identification risk.



AI-driven decision systems

Advanced analytics and agentic AI amplify the use of data, increasing both opportunities and potential harms.



Central banks are no longer protecting databases. **They are governing interconnected data ecosystems.**

From Local Risk to **Systemic Data Risk**

A changing reality: from isolated incidents to interconnected risk across the ecosystem.

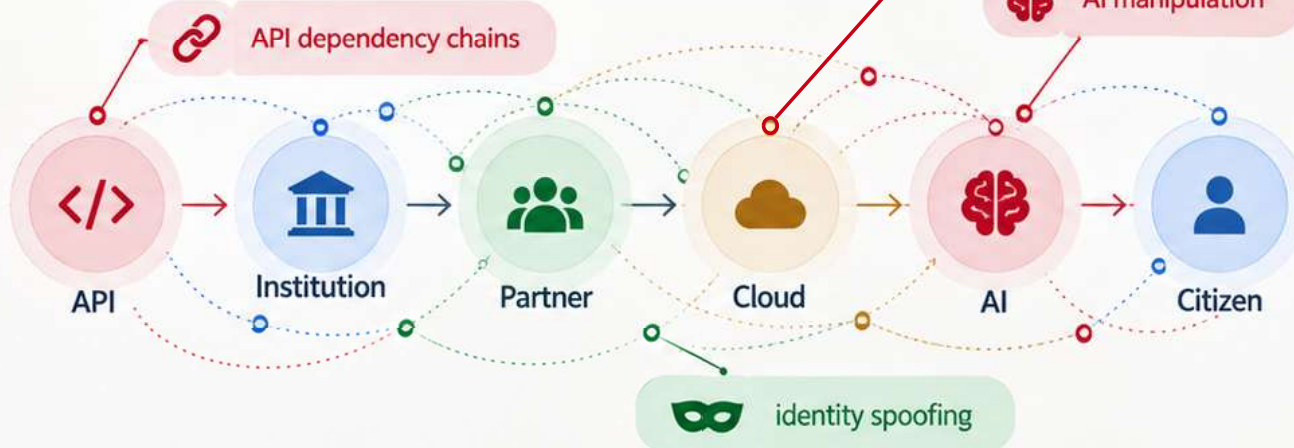
The old mental model

A localized and contained view of risk.



The new model

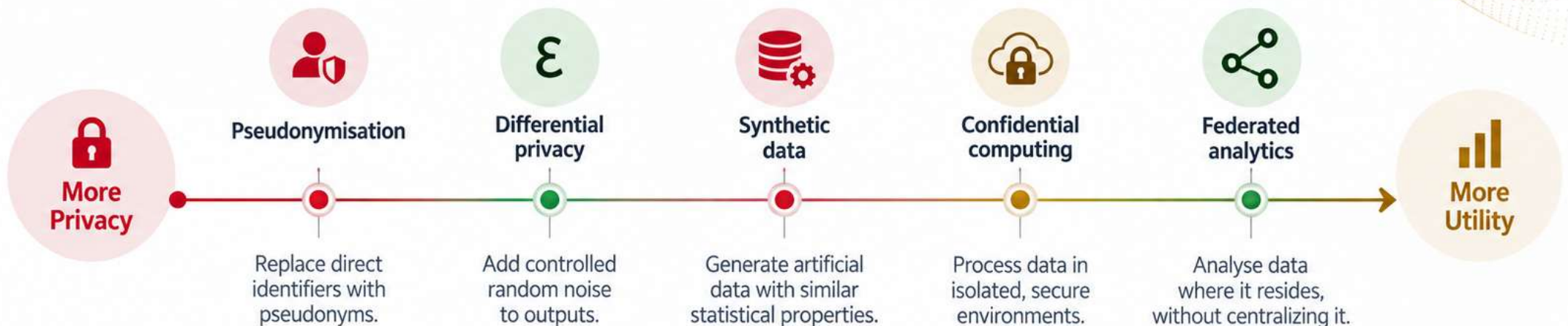
Risk propagates across an interconnected data ecosystem.



Risk is no longer localized. **It propagates across institutions.**

The classical **privacy-utility** trade-off

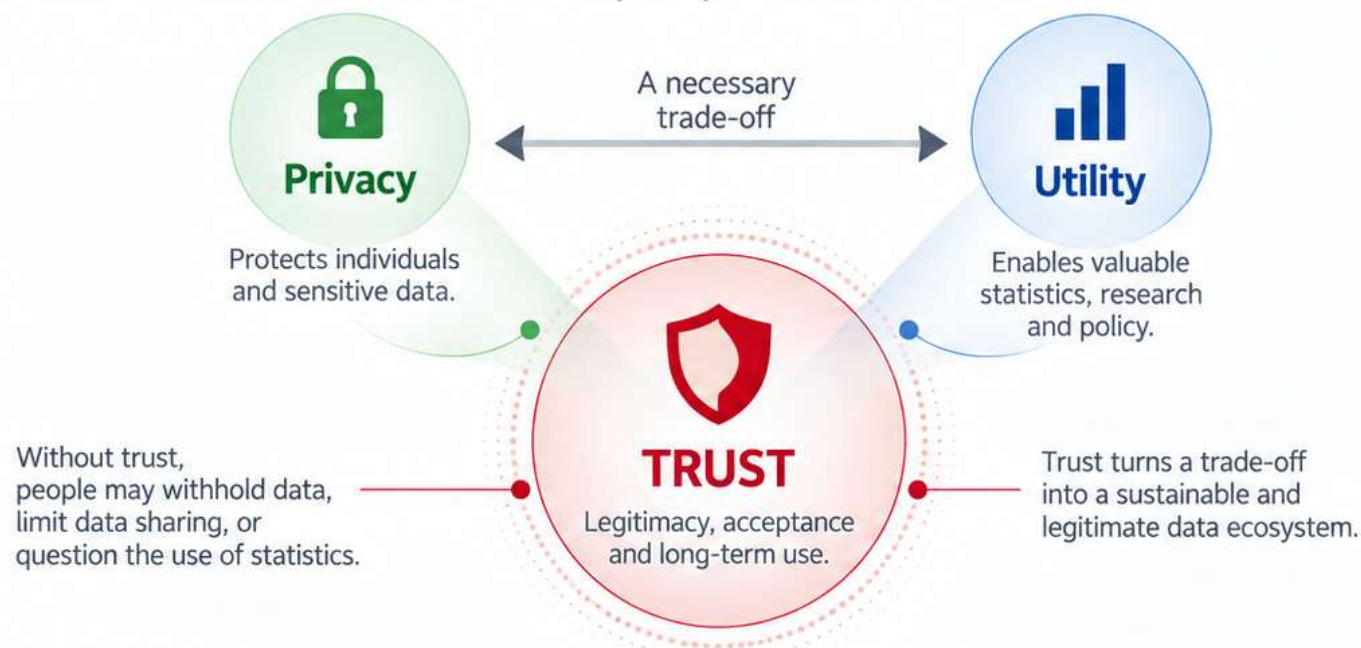
A range of technical tools to navigate the balance between privacy and utility.



We have become increasingly sophisticated at **optimizing privacy and utility.**

But something is **missing**

From a trade-off to a broader perspective.



“

Technical mechanisms can reduce exposure. They cannot, by themselves, **resolve the trust deficit.**

”



Privacy and utility are essential. But **trust is what makes them work** — in practice and over time.

Security is **not** trust



SECURITY



Is the system protected?



Controls



Confidentiality



Integrity



Access control



Objective/technical assurance



TRUST



Do I believe the institution will use my data appropriately?



Expectations



Fairness



Transparency



Legitimacy



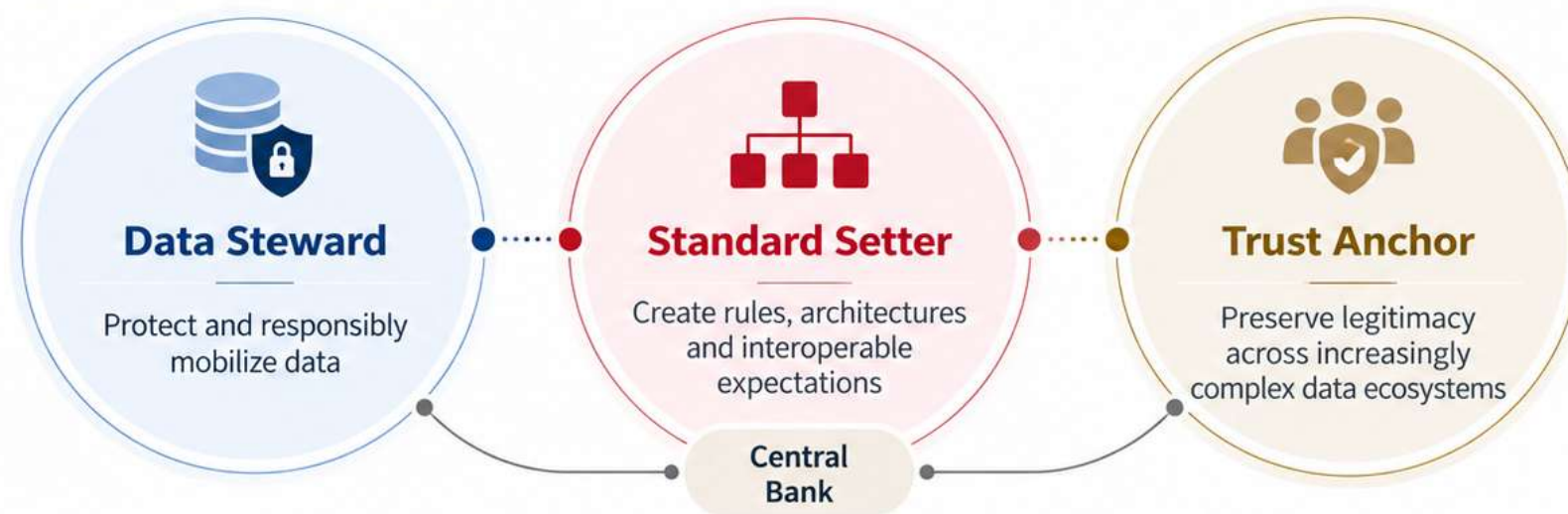
Perceived/institutional assurance



A system can be **highly secure** and still be **deeply distrusted**.

The role of the central bank **is changing**

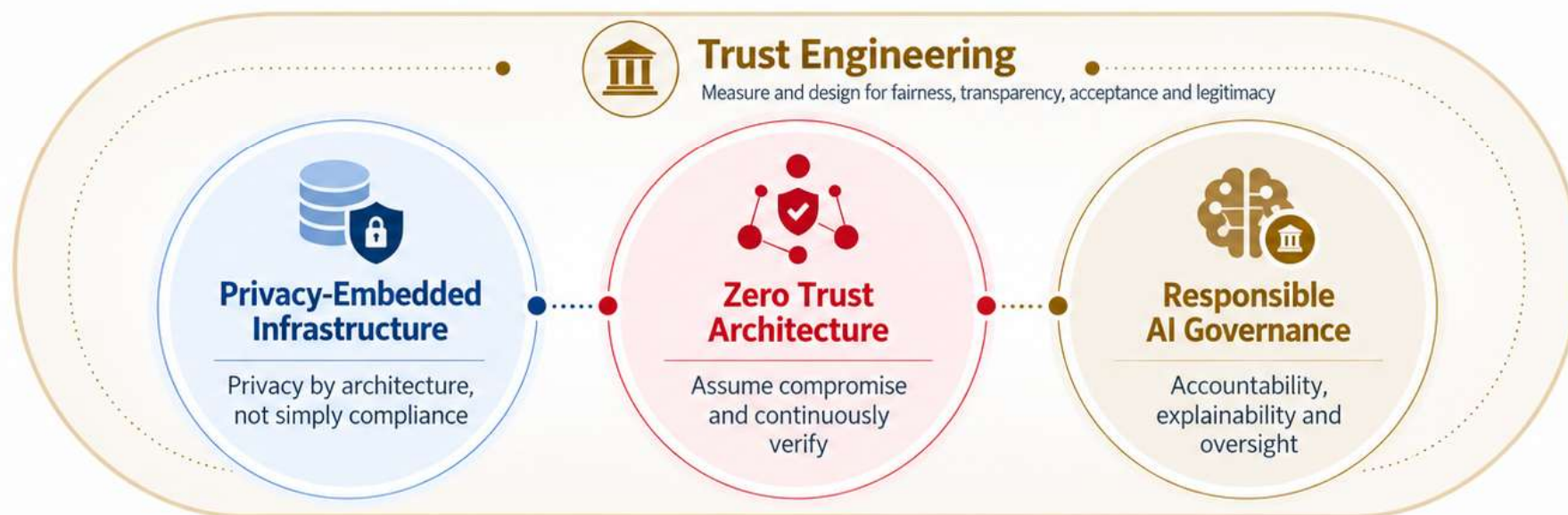
From data custodian to trust architect



Central banks cannot be only data custodians or regulators.
They increasingly become **architects of trusted data ecosystems**.

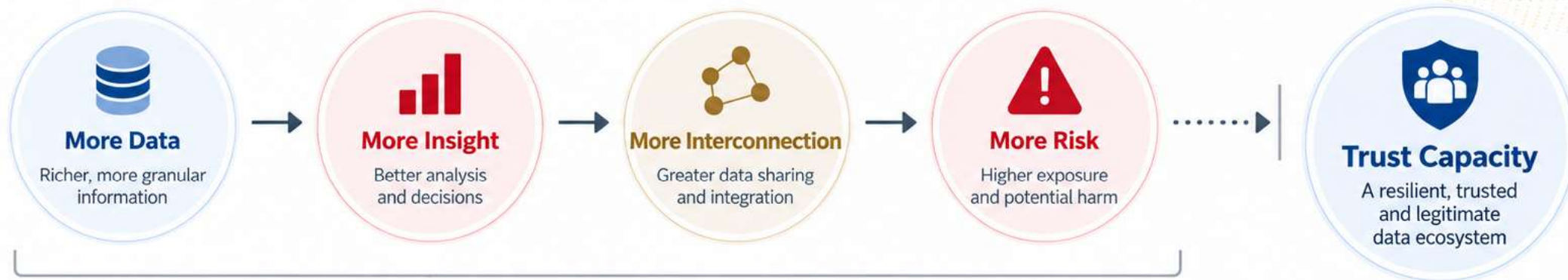
Four capabilities for **trusted data ecosystems**

The first three are established capabilities. The fourth makes legitimacy explicit.



Privacy, zero trust, and AI governance reduce exposure. **Trust engineering ensures legitimacy.**

The Data-Trust Paradox



Innovation capacity must grow **together with trust capacity.**



“The future of financial innovation will not be determined by how much data we collect, but by how much trust we preserve while using it.”



Would citizens accept a system that is perfectly secure, but feels **fundamentally intrusive**?

Thank You

Questions and Discussion

“ Without **trust**, even the most secure
data ecosystem will eventually
lose legitimacy. ”

Trust is what turns data use into legitimate public value.

Dr. Yasser Alhelaly