From Raw to Protected

Our journey to

Data Scrambling@ZEISS

Agenda

Agenda

It all started with one question:

How can we safeguard our test data without losing its power?

Challenge: Balancing data privacy with usability

Objective: Implementing a solution that protect data integrity while maintaining its value for testing.
Combines protection and usability.

Approach: Leveraging technologies and strategies that ensure data security without compromising functionality.

Agenda

Why we took action:
The urgency behind this mission

Consideration of GDPR

Data Scrambling decreases the probability, that personal data will be compromised

The process of data scrambling serves to mitigate the risk of re-identification of personal data

Reduce potential legal and financial liability

Keep reputation and customer trust intact by avoiding damages and losses

The Vision: Protecting data & trust

Data Scrambling as a core enabler for Digital Excellence

Core Enabler: Building the **foundation** for **secure Digital Transformation**

Drives secure and resilient digital transformation

Establishes the foundation for future data protection

Fosters trust and transparency across all digital initiatives

Agenda

Knowing what we want:
A solution that delivers both protection and usability

Functional Requirements

- Usefulness & functional fit
- Architectural fit & integration
- Compliance & validation
- Easy Customizing (preferred in SAP system)
- Adapter to non-SAP systems need to exist
- Addition of same logic in non-SAP standard tables
- Easy user-interface / Batch planning for execution or report / action

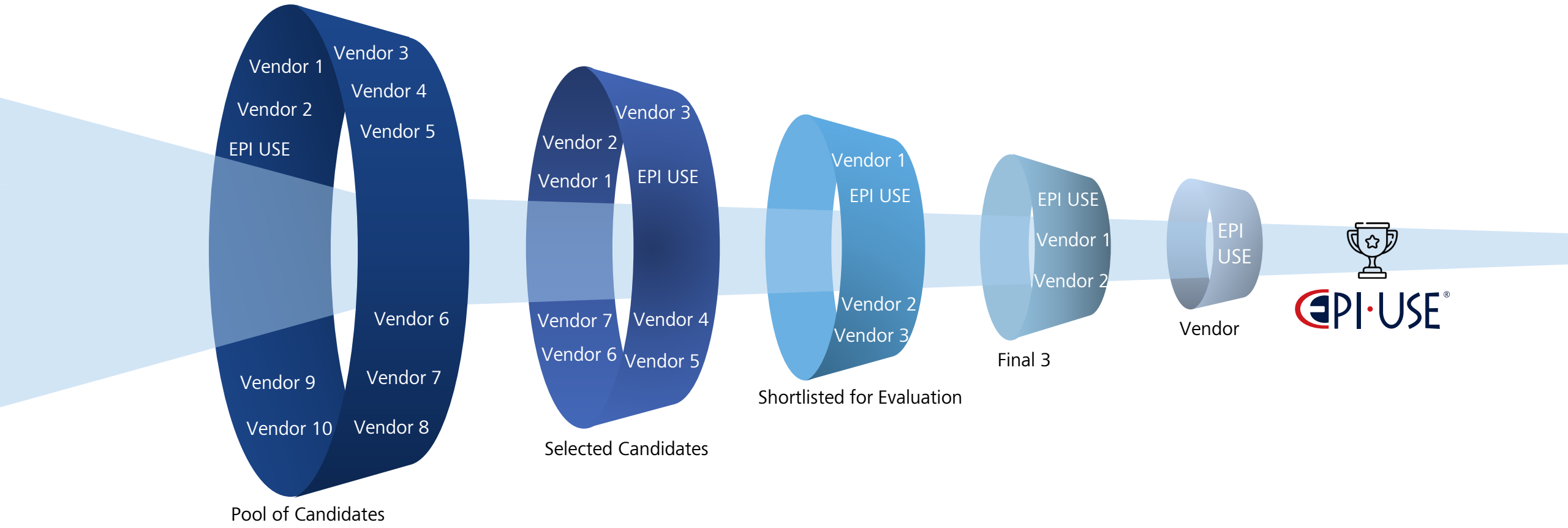
Data Privacy, Security and Quality

- Anonymization methods
- Meet the legal requirements (no more personal data is identifiable)
- Probability of Re-identification
- Type of data related to anonymization method
- Type of anonymization
- Anonymization with consistent key in different objects within multiple systems
- Cross-system anonymization
- Maintenance of Data Quality

Support and Scalability

- Vendor company & support & roadmap
- Toolset must be globally suitable

From a broad pool to the final choice:
A structured vendor evaluation process



Agenda

The Kick-Off: Igniting Change

From idea to execution

Project objectives

Consideration of GDPR

The process of data scrambling serves to mitigate the risk of re-identification of personal data

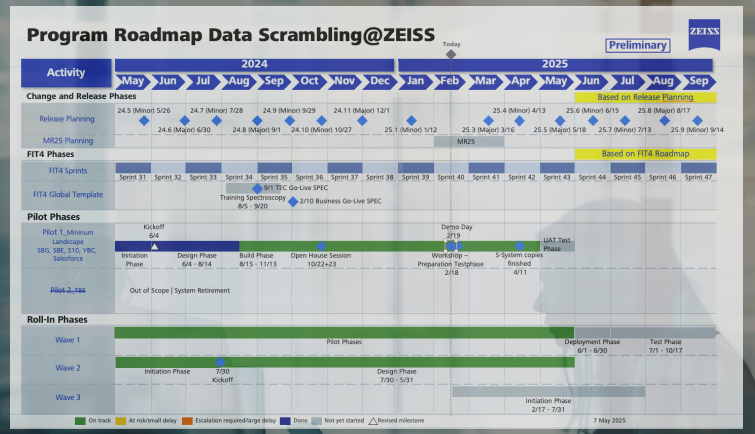
Data Scrambling decrease the probability that personal data will be compromised

Reduce potential legal and financial liability:

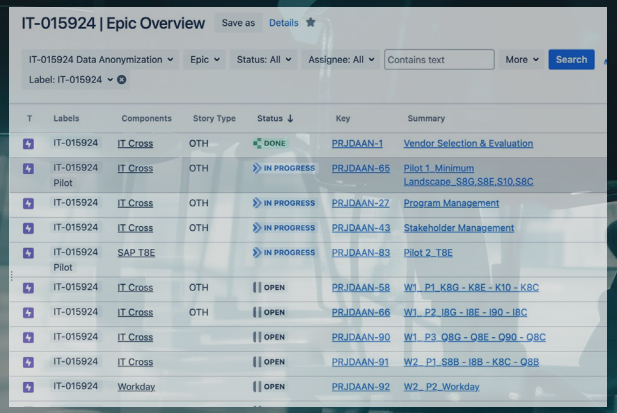
Up to 4% of yearly revenue of ZEISS Group for breaching GDPR law and negative impact on business operations and revenue.

Keep reputation and customer trust intact by avoiding damage and loss

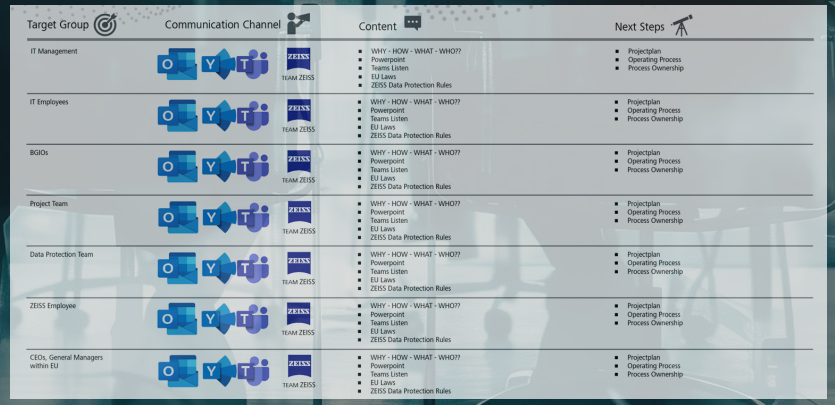
Roadmap



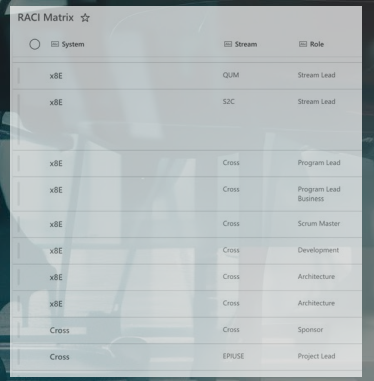
Deliverables



Communication Strategy

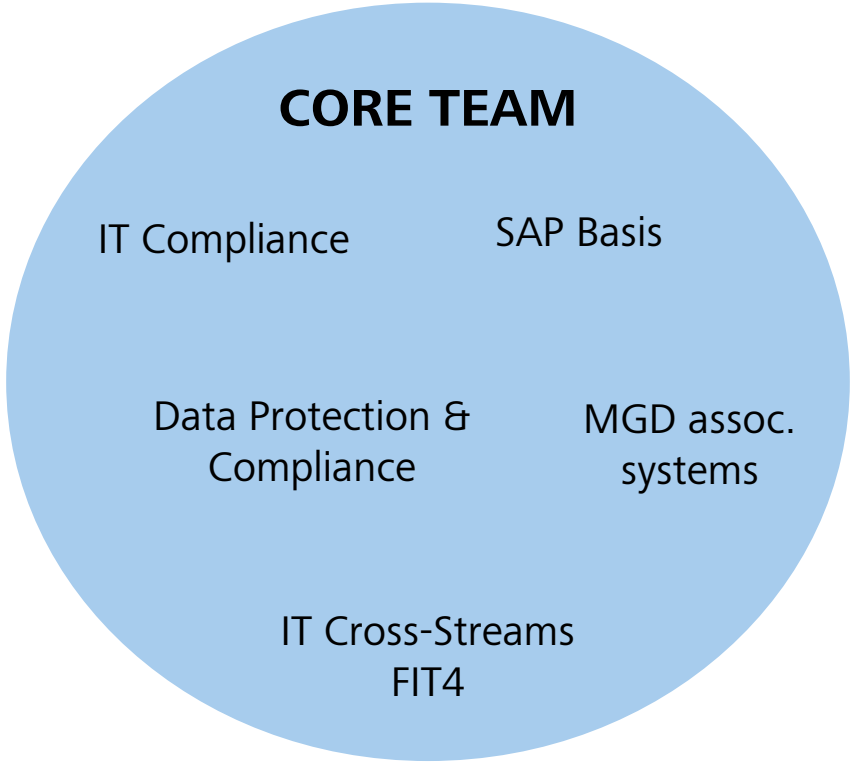


Roles and Responsibilities



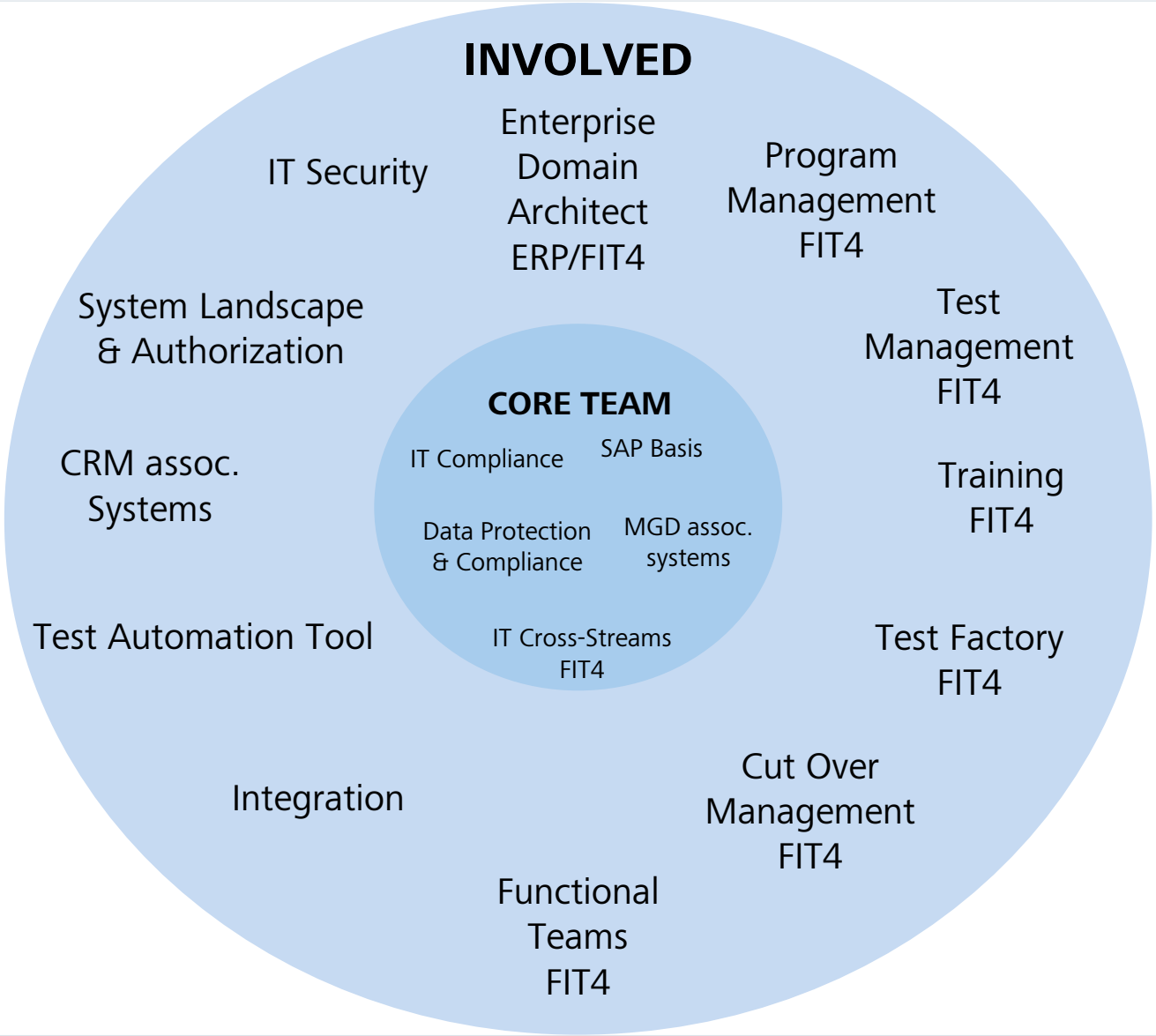
Identifying the right stakeholders

Clear roles and responsibilities across decision making and support functions



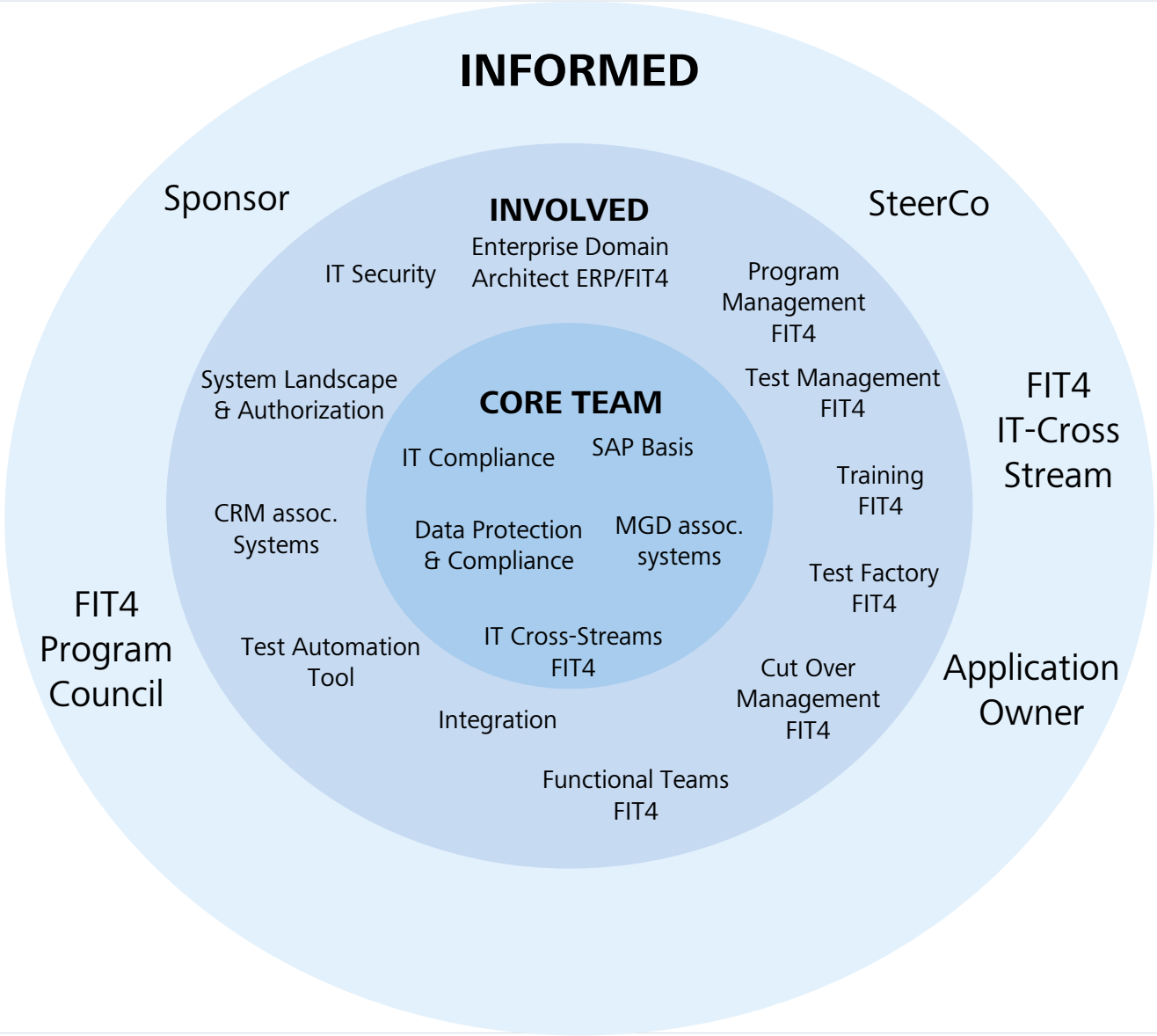
Identifying the right stakeholders

Clear roles and responsibilities across decision making and support functions



Identifying the right stakeholders

Clear roles and responsibilities across decision making and support functions



Agenda

Uncovering the landscape

Identifying systems and data fields in scope for scrambling

Comprehensive analysis of the **complex system landscape** to **identify** all **non-productive systems** within scope.

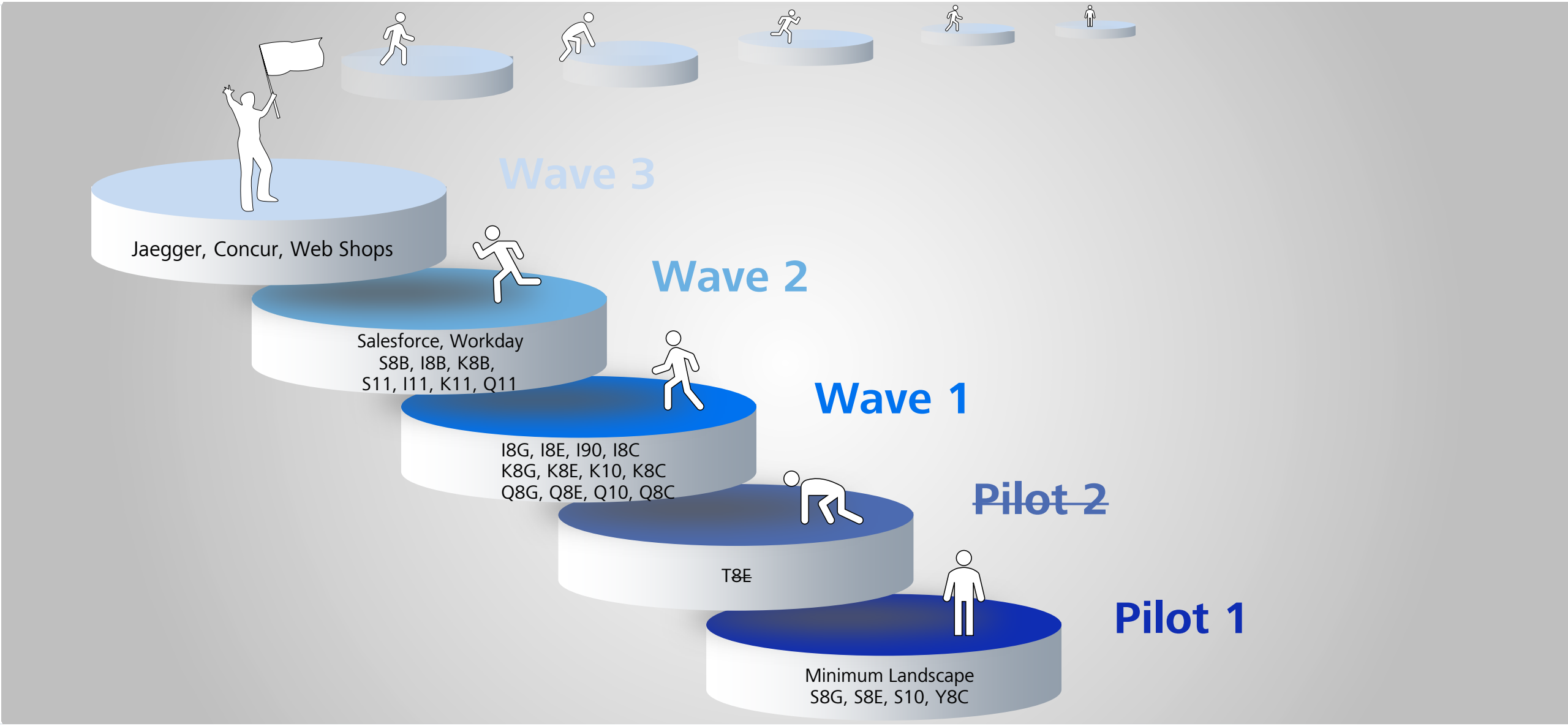
Detailed examination of **data objects** within each **system** to understand **data structures** and flows.

Collaborative decision-making with **stakeholders** to **determine** which **data fields** require **scrambling** (contact information, address information, financial information, personal identification information)

Establishment of clear **guidelines** for **data scrambling** across **identified systems**.

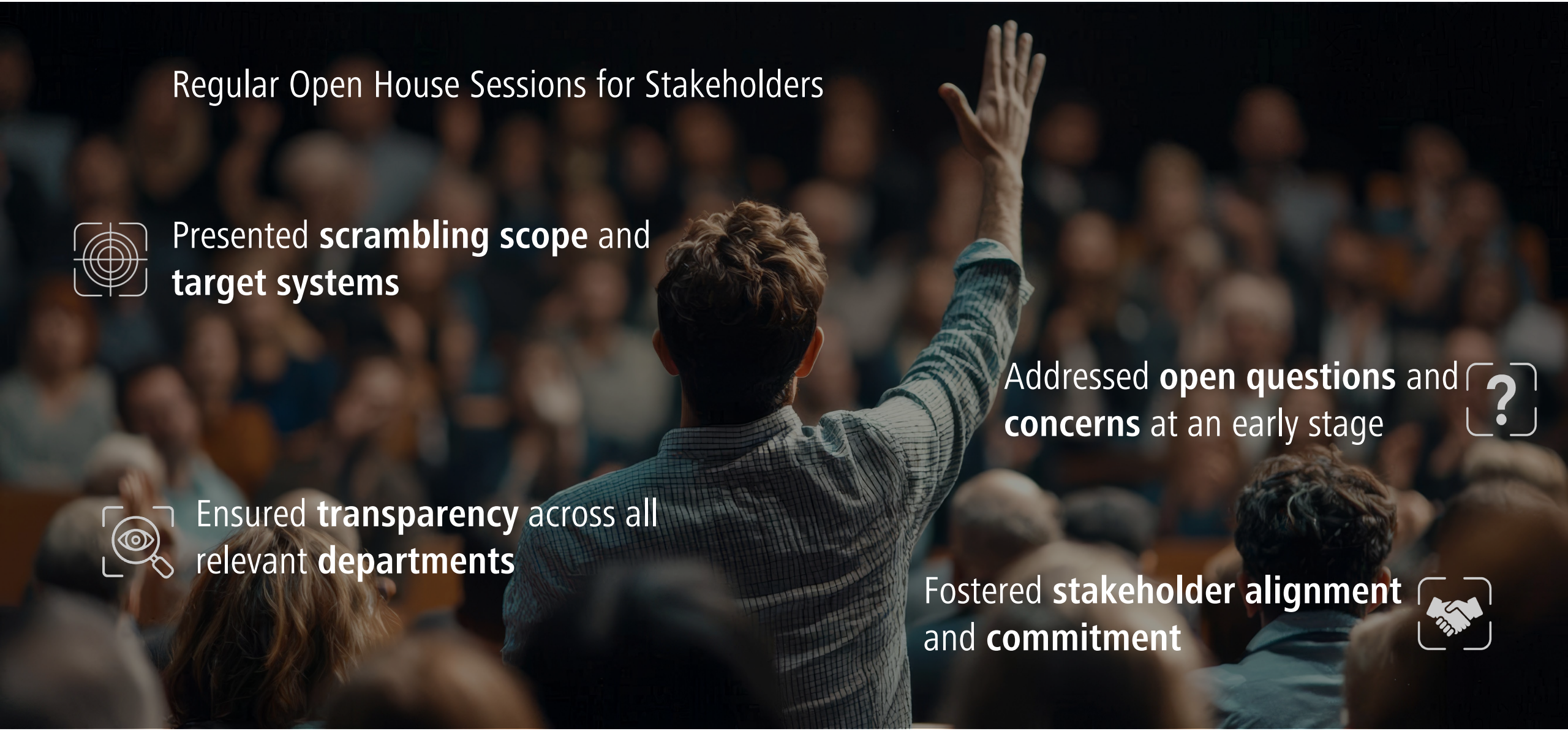
Step by step implementation across pilots and waves

Structured rollout from pilot phases to full implementation



Agenda

Continuous Alignment:
Collaboration and communication as the key to success



Agenda

Lessons Learned:
What we would do again? What we would do differently?

Start with alignment – involve Legal, Compliance early – don't wait until rollout

Don't underestimate complexity – every system, every data field has unique logic – generic scrambling fails

Not just on IT topic – business units must be part of the progress

Transparency pays off – regular updates and demos built stakeholders trust

Testing is not optional – data must remain technically correct and business relevant after scrambling

Think beyond today – build reusable logic & libraries for future projects from the beginning

Agenda

01 Introduction & background

02 The vision behind the project

03 Our requirements & the vendor selection

04 Project kick-off & stakeholder management

05 System analysis & implementation

06 Communication & change management

07 Lessons Learned & best practises

08 Outlook & Scaling

Outlook:
Anonymization as a foundation for the future

Anonymization enables **compliance** without compromising **insights**

It builds **trust**, ensures **legal certainty**, and empowers **scalable automation**

Develope a scrambling engine to integrate future systems

Data protection is **not** an **afterthought** — it's the **foundation**

Privacy-first architecture is the **backbone** of every **future-proof system**

In **process-driven organizations**, **anonymized data** fuels **safe innovation** and **smart decision-making**

Seeing beyond