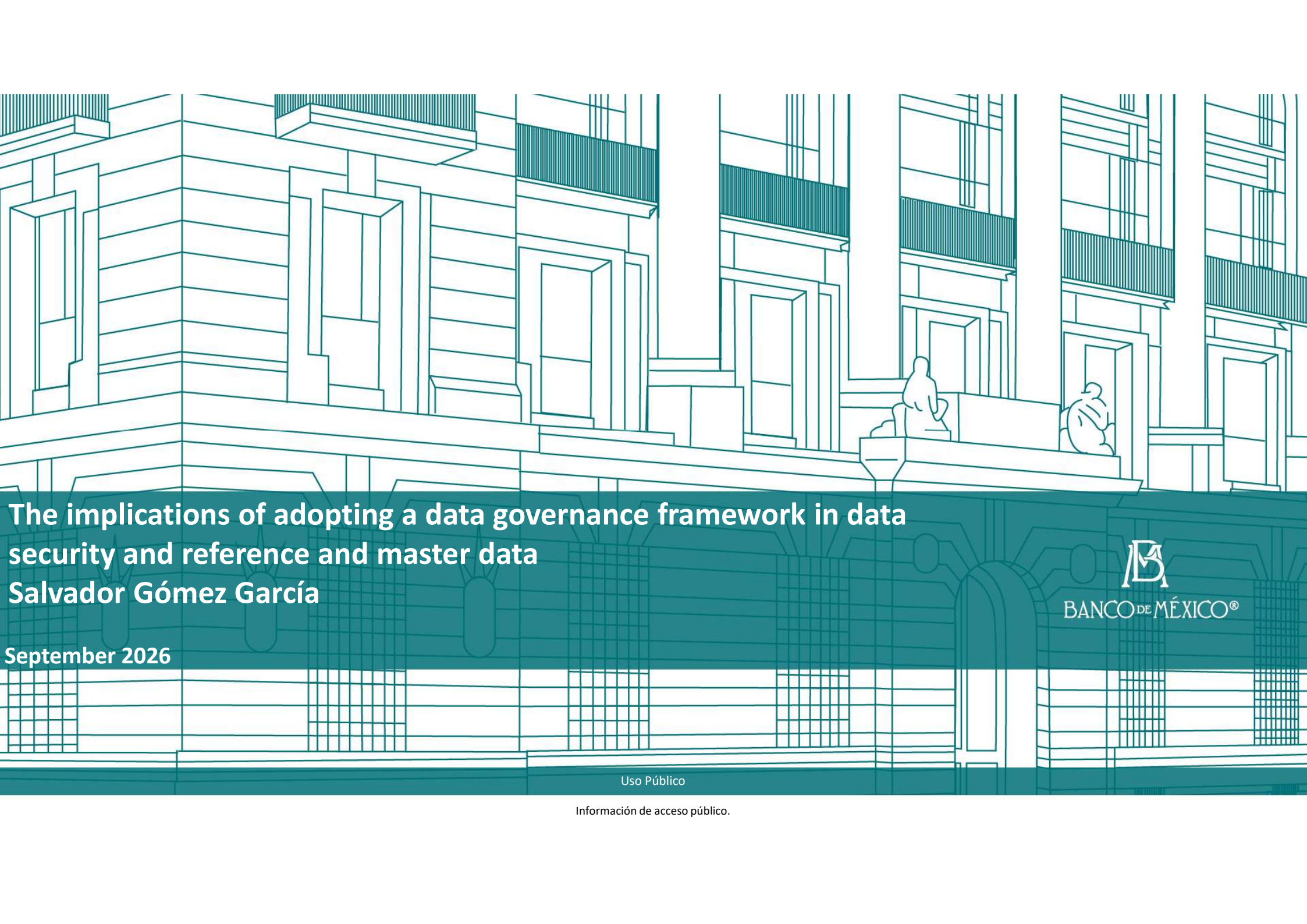




The implications of adopting a data governance framework in data security and reference and master data

Salvador Gómez García

September 2026



Uso Público

Información de acceso público.

PROGRAM

- Introduction
- The situation
- Aim and subjects
- DAMA as a solution
- Data Security
- Reference and Master Data

INTRODUCTION

- What is a data governance?
 - It has become a standard structure in many organizations.
 - It is the scheme of decision rights, processes, policies, standards, and roles.
 - It ensure data is: accurate, secure, available, compliant, consistently defined and used responsibly.
- What is a data governance framework?
 - It is a structured model that defines how governance is implemented across an organization.
 - With strategy the importance of robust metadata and data catalogues when managing sensitive data.
- What is DAMA?
 - Data Management Body of Knowledge is a framework.
 - The comprehensive data management best practices.
- What is Data Security?
 - Definition, planning, development, and execution of security policies.
 - Procedures to provide proper authentication, authorization, access, and auditing of data and information assets.
- What is Reference & Master Data?
 - Managins shared data to meet organizational goals.
 - Reduce risks associated with data redundancy.
 - Ensure higher quality.
 - Reduce the cost of data integration.

THE SITUATION

- After the outbreak, the DISF (Directorate of Financial System Information) has had a lot of information related to Data Governance.
- The DISF has had diverse policies, rules, methodologies and so on.
- The DISF has had the knowledge and certain experience how to manage the Master Data and Data Security.

AIM AND SUBJECTS

- The importance to implement a formal Data Governance inside of the DISF.
 - The adoption of one of the major standards Data Governance Framework, depending of the challenges of the DISF: DAMA-DMBOK, DCAM, COBIT, CMMI DMM, DGI Framework.
 - The challenges in the Data Security and Master Data.
 - The participation of a third party.

DAMA as a SOLUTION

Aim of the project

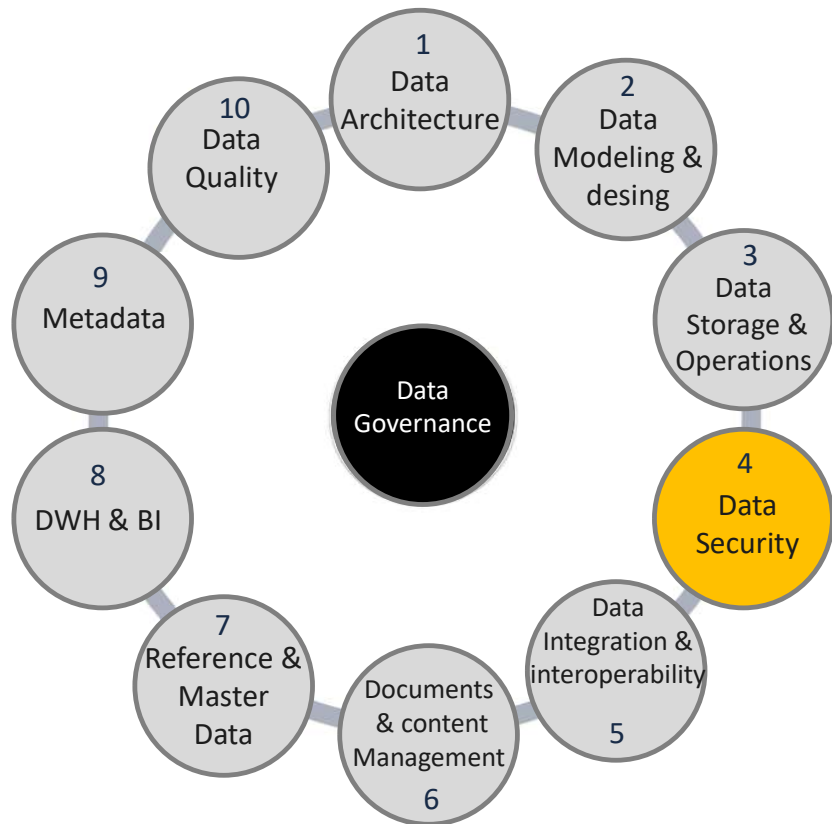
To adopt the DAMA framework at the DISF in order to harmonise, standardise, evaluate and implement improvements to the DISF's current data management processes.

To achieve this, the following steps will be taken for each discipline:

- A review of the current implementation of the DISF's data management processes to assess the extent to which they align with the various DAMA disciplines.
- Identify initiatives to improve this alignment.
- Set out projects and priorities for implementing the initiatives identified.
- To establish an initial **Data Governance** framework within the DISF that enables the setting of general guidelines for the design, storage, processing, modification, security, quality, traceability and description of data, to ensure the smooth operational functioning of the organisation.
- To assess the effectiveness of the measures implemented.

DATA SECURITY

DAMA Data Management Framework



Overall objective: Definition, planning, development, and implementation of security policies and procedures to promote appropriate authentication, authorization, access, and auditing of data and information assets.

Specific objectives:

1. Enable appropriate access to and prevent unauthorized access to corporate data assets.
2. Ensure compliance with regulations and policies regarding privacy, data protection, and confidentiality.
3. Ensure compliance with regulations and policies regarding privacy, data protection, and confidentiality.

DATA SECURITY

Assessment

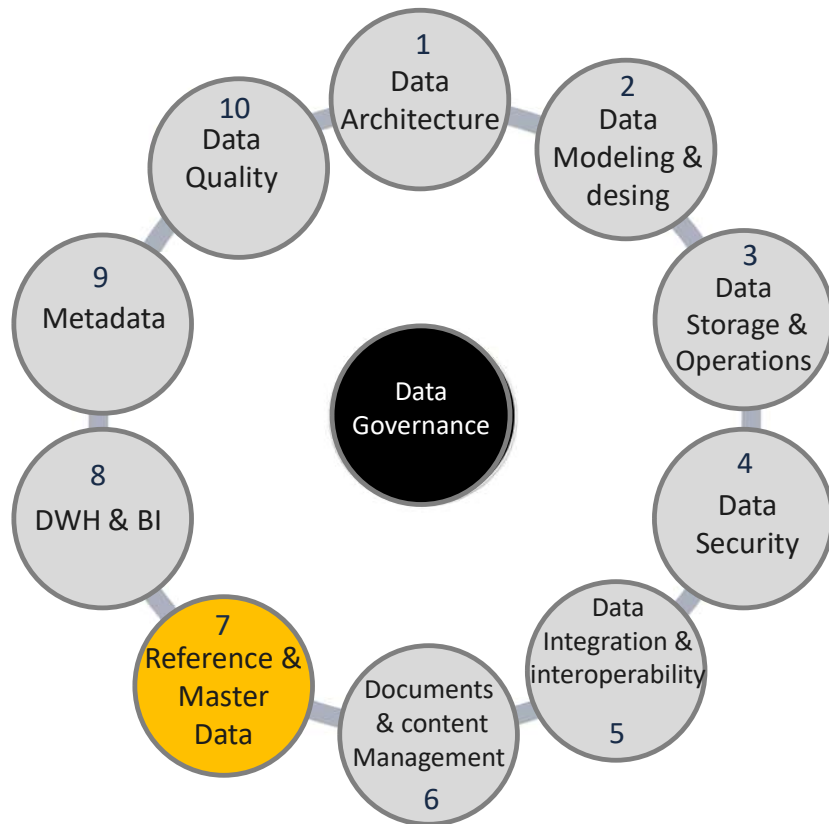
Score	Dimension DS	Practical Work	Level	Rating
83%	Security requirements	Requests arising from threats or incidents	Medium	50%
		Managing human-factor risks	Highlighted	100%
		Security agenda covering business areas and the board of directors	Highlighted	100%
67%	Enterprise security architecture	Impact of the expansion of the cybersecurity network	Highlighted	100%
		Improvements to the architecture in response to new types of risk and new technology	Medium	50%
		Assessment of integrated security tools (e.g. cloud-based and as a service)	Medium	50%
90%	Security metadata	Scope of the privacy and confidentiality classification labelling tool	Advanced	90%
		Metrics on compliance with data processing requirements by classification	Advanced	90%
		A culture of information classification and processing	Advanced	90%
90%	Security policy and standards	Policy coverage across the entire digital supply chain	Advanced	90%
		Analysis of the effectiveness of communication and training on safety policies and standards	Advanced	90%
		Agility in updating security policies and standards at bank level	Advanced	90%
77%	Security measures put in place	Assessment of opportunities for the automation of security controls	Advanced	90%
		Metrics relating to security control breaches or exceptions	Advanced	90%
		Government in the inventory of security controls	Medium	50%
93%	Security audits	Level of maturity of cyber risk assessment in the bank's various areas	Advanced	90%
		Prompt handling of security audit findings	Advanced	90%
		Completeness and use of audit-derived security control compliance metrics	Highlighted	100%
83%	Advanced/Sustainable			

DATA SECURITY

ID	Initiative	Priority (Stage)
1	To create and maintain a list of new security requirements (security backlog) arising from threats or incidents, describing the corrective actions taken to address them	Stage 1
2	Establish a formal and regular assessment of new threats, based on a cyber risk assessment of trends and new attack and defence technologies	Stage 1
3	Assess the level of effort and consistency in implementing security measures using the various tools currently available (this will help to compare them with other integrated cybersecurity solutions)	Stage 1
4	Compile a list of controls and keep it up to date, including details of the relevant governing bodies (who authorises them, who can request changes, when they are reviewed, etc.)	Stage 1
5	Obtain regular metrics on breaches and requests for exemptions from security controls, and carry out the necessary analysis to ensure these remain within acceptable limits	Stage 3
6	To increase the use and awareness of the labelling tool and ensure that labels accompany classified information	Stage 2

REFERENCE AND MASTER DATA

DAMA Data Management Framework



Overall objective: To manage shared data in order to understand organisational objectives, reduce risks associated with data redundancy, ensure high quality and reduce the costs of data integration.

Specific objectives:

1. To ensure that master and reference data is complete, consistent, up to date and authoritative throughout the organisation's processes.
2. Enable master and reference data to be shared across business functions and applications.
3. To reduce the cost and complexity of using data, and to integrate it through standards, common data models and integration patterns.

REFERENCE AND MASTER DATA

Assessment

Score	Dimension MDM	Practical Work	Level	Rating
75%	Maintenance of identity and association rules (quality)	Systematic review of business rules affecting master data	Advanced	90%
		Controlled changes to master data	Advanced	90%
		Approval and maintenance of master catalogues	Highlighted	100%
		Updated metadata in use for master data	Minimum	20%
80%	Management of update and exchange flows (government)	Standard for handling master data requests	Advanced	90%
		Established master data management processes	Advanced	90%
		Definition of functions for master data	Advanced	90%
		IT and business synergy for master data governance	Medium	50%
90%	Resolving conflicts arising from incorrect associations (discrepancies)	Managing the complexity associated with master data	Advanced	90%
		Handling incidents relating to master data	Advanced	90%
		Facilities for auditing and rectifying errors in master data mapping	Advanced	90%
		Regular review of business uses for master data	Advanced	90%
90%	Management of stakeholders in the workflow (responsibility)	Clear roles for master data management	Advanced	90%
		Level of implementation of master data functions	Advanced	90%
		Assignment of authority at organisational level regarding master data	Advanced	90%
		Level of business involvement in master data change management	Advanced	90%
93%	Architecture, tools and automation (technology)	Master data architecture enabled	Highlighted	100%
		Tools tailored to business needs for master data	Advanced	90%
		Level of automation in master data update and exchange processes	Advanced	90%
		Technological innovation to improve master data management	Advanced	90%
93%	Notifications of changes to users and applications (sharing)	Communication process established for changes to master data	Advanced	90%
		Exchange hubs authorised for the organization	Highlighted	100%
		A sharing process that is established and aligned with business needs	Advanced	90%
		Access level for master catalogue information	Advanced	90%
87%	Advanced			

Uso Público

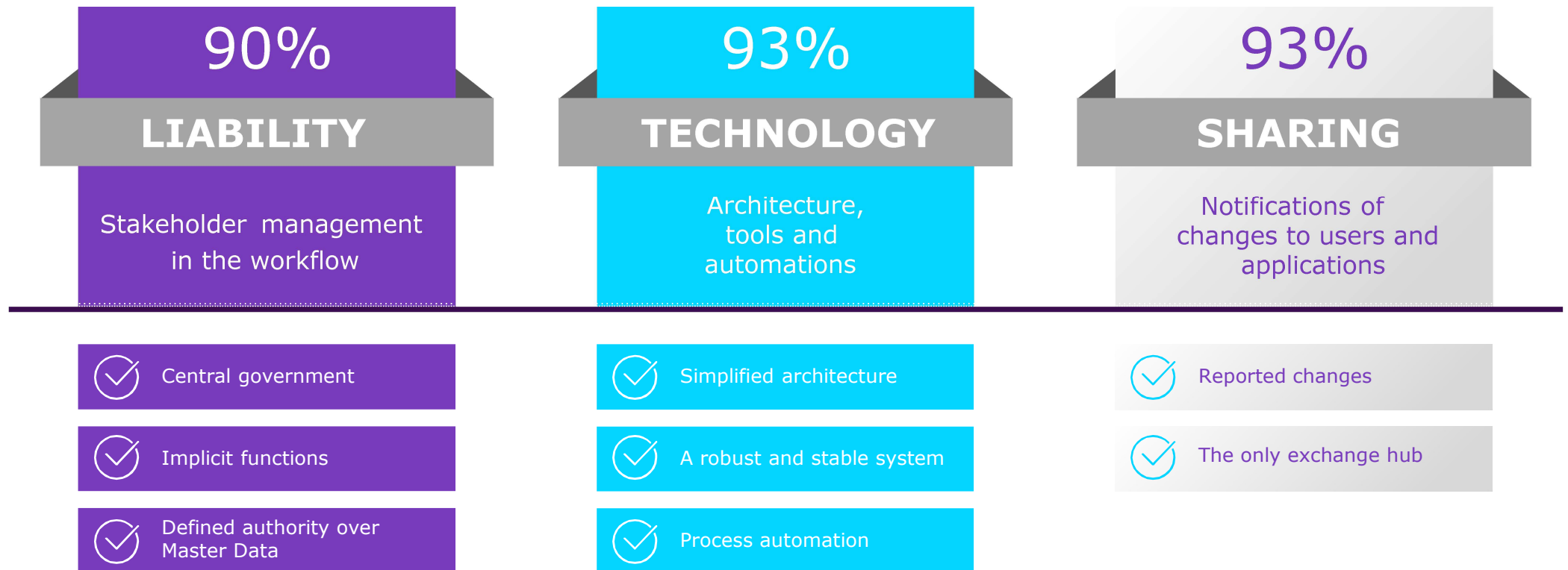
11

Información de acceso público.

REFERENCE AND MASTER DATA

Assessment

Level of compliance with practices



REFERENCE AND MASTER DATA

ID	Initiative	Priority (Stage)
1	Audits planned to verify the validity and quality of Master Data and its rules	Stage 1
2	Assess and define activities to integrate the business with master data functions (e.g. dissemination, raising awareness, business value, etc.).	Stage 2
3	Ensure clarity within the Master Data management process regarding the activities and persons responsible for creating, updating and sharing master data (ensure that best practices are followed)	Stage 3
4	Consider changes or improvements to Master Data management tools in the technology roadmap. Analysis of the backlog of improvements	Stage 1
5	Improve the definition and communication of changes to catalogues (reasons, impact and new usage)	Stage 3
6	Generate and maintain specific metadata for Master Data and ensure it is published	Stage 2
7	Develop content on updates to Master Data and share it across the organisation (portal, apps, automated notifications)	Stage 3

THANK YOU!

Questions & Answers



BANCO DE MÉXICO®

www.banxico.org.mx

Información de acceso público.