Data Architecture Standard

Standard owner:	Chief Operating Officer
Standard approver:	Executive Committee
Approval date:	2nd May 2023
Annual review date:	April 2024
Document owner:	Managing Director, Data Management Office.

1. Purpose

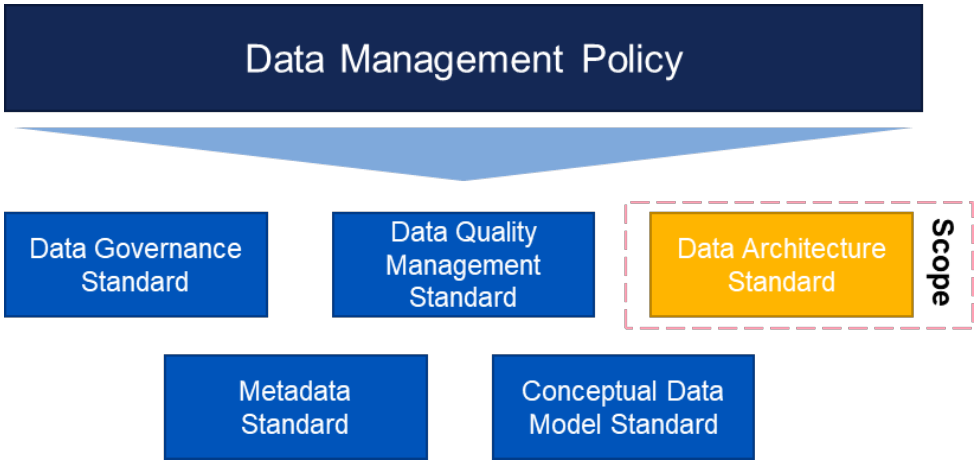
1.1 Purpose

This Data Architecture Standard was defined to drive a consistent understanding of data architecture across the bank. The document will serve as the foundation for strategic decisions related to the Bank's data architecture.

The adoption of this standard is mandatory to ensure that the implementation of the Data Management Policy in relation to Structured Data ("the Policy") is carried out appropriately and consistently across businesses functions at BBB.

This document covers the following aspects:

- **Data architecture principles and guidelines and associated documentation requirements for change activity at BBB to demonstrate adherence to the principles**
- **The role of relevant oversight and review bodies in ensuring adherence to the Data Architecture Principles and Guidelines**
- **Data source categories and associated data architecture standards**
- **Key accountabilities and responsibilities that need to be followed by the data governance role holders to carry out data architecture activities.**



2. Scope

This Policy and the associated Standards, apply to all BBB entities, operations, subsidiaries, and Colleagues (see Appendix A Policy Scoping, Policy Governance Framework for definitions) and interactions with Structured Data ("data"), from origination to processing, reporting and analytics.

Note: The Bank's Data Protection Policy and Information Security policies relate to issues of data protection and security, therefore are not covered in the Policy.

3. Key Requirements

3.1 Data Architecture Principles and Guidelines

The data architecture principles and the associated guidelines inform the evaluation and design of changes and solutions, with the goal of driving towards a target state data architecture that exhibits simplicity, supports data quality, accessibility, and trust in data, and facilitates effective data management.

Data Architecture Principle	Guideline
Simplicity and Agility	Architecture design should ensure there is no duplicate capture of the same data points
High Quality and Trusted Data	Architecture should support the capture of metadata and data lineage and source input data from designated systems of record
	Architecture must align with standard data quality processes to ensure the integrity of the data
Accessibility of Data (for those who should have access)	Data integrated with downstream applications enabling ease of data discovery and retrieval
	Architecture must govern access permissions
	Architecture should provide an easy-to-use interface for data consumption by end users
Good Data Management Practices	Architecture must establish automated data supply chains to promote sustainable and efficient solutions by replacing manual EUC's
	All data used should originate from trusted sources
	Architecture should aim to eliminate departmental data silos and promote collaboration wherever suitable to ensure all stakeholders have access to high quality, trusted data with complete metadata
	Certain scenarios require that data cannot be shared across departments (e.g., subsets of SUL data) – architecture must comply with appropriate rules pertaining said data.
	Data ownership must be established for increased accountability of data assets
	Architecture must contain a comprehensive metadata tool to capture and maintain metadata across the organisation, enabling improved transparency for critical data elements and processes
	All systems underlying architecture landscape must comply with governance principles
	The level of security required for data should be considered and any solution implement required controls e.g., if it contains PII, CIA principles etc.
	Architecture design must take full consideration of policies and controls required
Conformance	The data architecture designs and implementations must align with established enterprise data model designs and business terminologies.

3.2 Data Architecture Considerations with respect to Change Initiatives

Changes within BBB arise from different routes with varying levels of governance and standardised procedures. Changes include technology changes, product changes, process changes etc. and each follow different paths to implementation within BBB. Consideration of, and adherence to, the Data Architecture Principles and Guidelines must be evidenced for all changes as per the requirements set out in the respective tables below.

The role of relevant oversight and review bodies in ensuring adherence to the Data Architecture Principles and Guidelines is detailed in section 3.3. Oversight and Review Bodies.

3.2.1 Project Development Lifecycle (PDL)

PDL follows five stages of change implementation from Define to Deliver and Close. The change request details the business requirements which are analysed and if updates to existing technology or a new technology is not required, then the change follows PDL procedure.

The five stages in the PDL with associated data architecture standard requirements are as follows:

Stage	Description	Data Architecture Standard Requirement
Define	• To propose a researched business idea which aligns to strategic goals and enables to explore the idea further within some allocated time, budget and resources	• **High Level Data Assessment** questionnaire must be completed by the change requester to provide a broad overview of the impact of the proposed changes with respect to data • The responses to the high-level assessment must be reviewed by the Data Domain Owner and shared with the DMO • Data Architect must be included in the review of the change requests along with stakeholders from other domains • The change proposal must explain how the change will align to the Data Architecture Principles
Select	• To propose the most relevant approach to delivering the required business outcomes and to provide a business case which supports this approach	• **Detailed Data Assessment** must be completed to evaluate the business opportunity against the Data Strategy and Principles • The responses to the detailed data assessment must be collated with inputs from the Data Stewards of the relevant business function and presented with other relevant architecture documentation to the Architecture Review Board (ARB) • Resources, costs and deliverables must be identified with firm commitment for the next phase and this must include data resources where applicable
Design	• To have an approved design which has passed all relevant checks, and which underpins delivery, deployment and support plans and a business case that remains valid	• Revised Impact Assessments informs Deliver stage. Any mitigations identified in the detailed Data Assessment should be completed and approved • A business owner(s) and corresponding Data Owners have been identified to own and track benefits
Deliver	• To have a completed, tested solution which meets the agreed design and is ready for deployment	• Corresponding Data Owners should be made aware of the changes to be implemented pre-go live.
Close	• To have an implemented solution, utilised by the users and to demonstrate that the solution has achieved all benefits, to time, budget, and in a controlled manner.	N/A

3.2.2 Software Development Lifecycle (SDLC)

The business requirements detailed in the change request are analysed and if an update to technology or a new technology is required, then the change follows SDLC procedure, and the requirements must be submitted to governing forum for review. If approved, the SDLC process will be followed to deliver the changes and the project team must be kept up to date by the Technology Delivery Working Group.

The five stages in the SDLC with associated data architecture standard requirements are as follows:

Stage	Description	Data Architecture Standard Requirement
Define	• The beginning of the delivery where the requirements are explored • The functional and non-functional requirements are specified as clearly as possible. • Alignment to the IT strategy is confirmed – all technology updates must follow IT strategy principles • Resources are assigned to deliver the request based on priorities set by BBB's change prioritisation process	• **High Level Data Assessment** questionnaire must be completed by the change requester to provide a broad overview of the requirements and impact of the proposed changes with respect to Data • The responses to the high-level assessment must be reviewed by the Data Domain Owner and shared with the DMO.
Select	• Technology options are explored to deliver the request • Architecture principles, as detailed in the IT strategy, are followed • A technology option is chosen that will meet the requirements • If a new system is required, the procurement process is followed to purchase the new system	• **Architecture Vision Document** must be completed and used to review the business problem or opportunity, outline the business requirements and objectives, and begin to shape the high-level solution architecture. This should be aligned to the data and wider enterprise architecture principles. • **Detailed Data Assessment** must be completed to evaluate the business opportunity against the Data Strategy and Data Principles. • The Data Architect must collate the responses to the detailed data assessment with inputs from the Data Stewards of the relevant business area / function and present it along with other relevant architecture documentation to the Architecture Review Board (ARB) • **Key Design Decision** document must be used to choose a new provides all decisions, and this must include all data architecture related decisions • **High Level Design document** showing the main components that would be developed and their interfaces must be completed. This must include: ○ clear definition of data ○ data sources ○ data flow ○ data sharing and access requirements to/by third party ○ data security ○ data lifecycle (storage, retention, etc.)
Design	• The design documents will detail how the new system or system changes will meet the requirements • There are two design documents, a high-level design which is then used to produce a technical design	• **Technical Design Document** must be completed and must include all the information required to build or upgrade the new solution and how to integrate it with existing applications. This must include Data Model and field level Data change details along with Data Quality checks to be implemented – data input validations, reconciliation, etc. • Data Architect must be included in the list of stakeholders to review the developed solution before hand-off to testing team. • Test report documents must be produced by testing team and reviewed by the Data Architect to ensure that the implementation has been completed as per the design.
Deliver	• Transform the technical design into a system to be tested • The system changes are tested to make sure they meet the requirements • After successful testing the new system or the system changes are moved from test into production.	• Corresponding Data Owners should be made aware of the changes to be implemented pre-go live.
Close	• Analyse performance after the delivery is complete	N/A

	• Post implementation review, lessons learned produced, any suggested updates to the procedure incorporated	

3.2.3 Product Development Committee (PDC)

The objective of the PDC is to make recommendations for both the introduction of new products/programmes and any material variations of existing products/programmes.

The stages in the PDC process with associated data architecture standard requirements are as follows:

Stage	Description	Data Architecture Requirements
Proposed product development changes are discussed at the PDC	New product requester needs to describe all requirements and templates and share views to the board relating to product development	• **High Level Data Assessment** questionnaire must be completed to provide a broad overview of the impact of the proposed changes with respect to Data • The responses to the high-level assessment must be reviewed by the Data Domain Owner and shared with the DMO.
Project Implementation Plan	Participants share views on product roll out where a pilot had been chosen to first implement a product.	* Timescales and resource requirements involving data architecture activities are clearly set out with risks to cost or time over-runs understood.
Detailed Review	Project owners will have to carry out in depth analysis in considering market gaps and failures in the market and produce design options, and a full business case proposal	• **Detailed Data Assessment** must be completed to be used to evaluate the business opportunity against the Data Strategy and Principles • The Data Architect must collate the responses to the detailed data assessment with inputs from the Data Stewards of the relevant business function and present it along with other relevant architecture documentation to the Architecture Review Board (ARB)
Recommendation to Board	The relevant MD will need to secure written sign-off by all relevant cross-Bank functions for their relevant aspects, following the checklists approved by the PDC.	• Architecture Team and DMO must be included **as part of the approval process.**

3.3 Oversight and Review Bodies

The following oversight and review bodies have a role in ensuring adherence to the data architecture principles and guidelines through consideration of the data architecture principles and standards as part of their decision-making process. There must be appropriate representation from DMO and Architecture teams to facilitate this.

3.3.1 Technology Request Forum

The Technology Request Forum aims to discuss and approve / reject change requests that have been identified as requiring a new software or technology.

Data Architects and DMO representation (relevant Data Domain Owner) must be included in the review of the change requests to ensure that any new technologies /changes to existing technology are aligned to data architecture principles and data source data architecture standards.

3.3.2 Architecture Review Board (ARB)

The ARB is to review and formally approve all architecture documentation (i.e., Architecture Vision, High Level Design and Technical Design documents and key design decision/option papers).

DMO representation (relevant Data Domain Owner) must be included in the ARB to ensure that the architecture vision is evaluated against the data architecture principles (informed by the Detailed Data Assessment).

3.3.3 Technology Delivery Working Group (TDWG)

This working group with representation from all key stakeholders is in place to manage the delivery of new technology. They review the Business Requirements and Architecture Vision and agree the best way to proceed. They are responsible for tracking delivery, reporting progress, and managing delivery risks.

Data Architects and DMO representation (relevant Data Domain Owner) must be included to ensure that any new technologies/changes to existing technology are aligned to the data architecture principles and data source data architecture standards.

3.3.4 Change Advisory Board (CAB)

CAB is the governance forum that will ensure all changes have been evaluated by the relevant stakeholders prior to approval or rejection, and to also review the success of implemented changes.

DMO representation must be included to ensure that the change is implemented appropriately as per the approved design and against the data management principles.

3.4 Data Source Categories and Standards

Five categories are defined for the designation of data sources, with the associated data architecture standards set out as follows:

Data Source Category	Descriptions	Impact	Data Architecture Standards
Systems of Insight (Consumers)	Provide the capability to analyse data and extract insight, based on data from across Systems of Record, Engagement and Control.	• Harness organisational data to generate insight. • Drive positive business outcomes with insight representing a key source of competitive advantage.	• System of Insight must have controls to ensure integrity with System of Record (Section 6 – Control Reference DM-003 and DM-004).
Systems of Engagement (Consumers)	Provide the capabilities and technology for users to engage with the organisation, including front end platforms for both clients and colleagues.	• Allows orchestration of simple, frictionless customer journeys. • Deliver customer-centric experiences through digitalisation of customer and colleagues touch points.	• System of Engagement must have preventative data controls if data input takes place within the system
Systems of Record (Producers)	Provide the platforms, technology, and engines to run core	• Traditional systems and applications. • Challenges with designating systems of record across	• System of Record must have preventative and detective controls as appropriate

	operations, handle business transactions and act as authoritative source for master data.	data domains and mastering data from across multiple systems of record.	• System of Record should enable mapping directly to related data in other Systems of Record through clearly defined key fields • Where systems meet the definition criteria for multiple different Data Source Categories, there should be clear logical separation of the different components within the platforms, e.g., data for which BI is the golden source vs. the System of Insight should be clearly identifiable. • System of Record must have data validation checks in
Systems of Control (Consumers)	Provide downstream monitoring and control systems and technology.	• Systems enable improved data governance through improved monitoring, automation, availability and understanding of data.	• Systems of Control should minimise the volume and longevity of data stored within the system, in line with the system's remit.
Systems of Ingestion (Producers)	Provide the layer for 3rd party data to be brought inside the organisation data landscape.	• Systems enable data quality principles of completeness, validity or uniqueness at origination , in order to detect potential data quality issues. •	• System of Ingestion must have data validation checks in place • Systems of Ingestion should adhere to standards defined as part of the Bank's strategy for API management and data integration.

The following standards are applicable across all data source categories:

- All business data should be made accessible on a least privilege basis, with system controls enforcing the relevant user permissions.
- Data storage should adhere to all provisions stipulated in the BBB records management policy.
- Data should be clearly classified according to BBB's data classification standards and suitable access controls applied.
- The data source must be providing the latest (fit-for-purpose) version of data records and be being actively maintained.
- The data source is linked to a published data element in the relevant metadata repository specifying Data Domain Owner, Data Owner, and Data Steward responsibility.
- The data source and its data element must be available within the Data Quality Issue Management (DQIM) tool so that data quality issues can be linked to both items and enter the BAU data quality issue management process.
- A Data Dictionary should be in place to describe data in the data sources, containing metadata on data sets, fields, relationships, definitions, etc. It can be Logical Data Dictionary (system agnostic, focusing on entities and fields) and Physical Data Dictionary (data in a specific database, focusing on tables and columns).
- The appropriate level of security standards must be applied to data when either in transit or at rest, this will include the enterprise adopted standards for encryption and security protocols.
- This standard must consider all other data management principles and standards, such as data quality, data governance, meta-data management & conceptual modelling.

3.5 Master Data Classification

New data introduced to or created by the bank must go through a screening process to determine if they are in scope for Master Data Management. This should be achieved through categorising the data into appropriate domains and concepts, assigning appropriate domain owners. This then prepares the data ready to be fed into appropriate logical and physical context to ensure alignment with respective guidelines. For guidelines and best practices in relation to Master Data Management, please see Reference and Master Data Management document.

4. Roles and Responsibilities

All colleagues with responsibility for the ownership, production and consumption of data are responsible for the integrity of the data, including reports and documents, under their control.

4.1 Data Domain Owner

Role and Accountability/ Responsibility
Data Domain Owners are Data Architects assigned by the Data Management Office to oversee one or more data domains. They are responsible for modelling, setting standards and approving definitions for data aligned to their data domain(s). They are involved in the change management process, challenging inputs in the Data Assessment Questionnaire, and attending and providing approval at relevant architecture and technology forums.
- **Responsible** for approving the mapping of data domains to data source(s) and approving the designation of System of Ingestion / Record / Engagement / Insight / Control. - **Responsible** for reviewing Data Assessments. - **Responsible** for participating in the Architecture Review Board, Technology Request Forum, Technology Delivery Working Group and Change Advisory Board to ensure proposed changes are appropriately evaluated against the data architecture principles.
-

4.2 Data Steward

Role and Accountability/ Responsibility
Data Stewards are responsible for management, control, integrity of data, and supporting data quality issue management and remediation.
- **Responsible** for identifying and proposing the designation of System of Ingestion / Record / Engagement / Insight / Control within their business area. - **Responsible** for supporting the completion of data assessments for changes related to their business area (in conjunction with change management and Data Architects assigned to change initiatives where relevant). - **Responsible** for identifying and cataloguing critical data contained within designated data sources owned by their business area.

4.3 Data Custodian

Role and Accountability/ Responsibility
Data Custodians are IT points of contact that are responsible for ensuring the accurate and controlled sourcing, transport, access, and storage of data at the application level.
- **Responsible** for implementing data controls for designated data sources in line with the standards requirements, e.g., detective data quality rules and preventative data quality controls such as input validation. - **Responsible** for maintaining appropriate system documentation for designated data sources in line with the standards requirements, e.g., data dictionary.

5. Further Reading

Further reading: Data Management Policy, System Development Lifecycle Procedure, BDA Data Architecture Modelling Standards, Business Architecture Canvas, Architecture Vision, Key Design Decision, High Level Design document, Technical Design document, Data Assessment Questionnaires, Information Classification Procedure, Reference and Master Data Management document.

6. Policy Controls

Controls in place regarding this policy are as follows:

Control Reference	Control Title	Description	Frequency
DM-001	Data Governance Roles	All business areas must assign a Data Owner and Data Steward. All systems must have an assigned Data Custodian. Each data domain must have an assigned Data Domain Owner.	**Continuous**
DM-002	Critical Data Elements (CDE) Identified and Under Governance	Critical Data Elements (CDEs) are data elements used for making business decisions that have an impact on the bank's financial performance, results, or bottom line. This control requires that CDEs must be defined and grouped within the business objects hierarchy with associated metadata, data sources, lineage and governance roles recorded and maintained.	**Continuous**
DM-003	Preventative Data Quality	Preventative data quality controls (e.g. input validations) must be implemented for critical data elements.	**Continuous**
DM-004	Detective Data Quality	Detective data quality controls (data quality measurement) must be implemented for critical data elements.	**Monthly**
DM-005	Issue Management	A data quality issue management process is in place.	**Monthly**
DM-006	Systems of record	System of Record is where the data is screened, managed, updated, deleted or mastered, validated and where exceptions are remediated.	**Continuous**

		This control requires that each CDE has a designated system of record (which cannot be an end-user repository) with appropriate controls, where the data is managed, updated, deleted or mastered, validated and where exceptions are remediated.	
DM-007	Data Assessment as part of Change Initiatives	Data Assessments must be performed as part of the evaluation and design of changes and solutions to ensure data architecture principles are followed.	**Continuous**

7. Definition of Terms

Term	Definition
BAU	Business as usual, the normal execution of standard functional operations within an organisation, forms a possible contrast to projects or programmes which might introduce change.
BBB or the bank	The British Business Bank plc ("BBB" or "the bank") and its subsidiaries.
Colleagues	Permanent Employees, Fixed Term Contract, Apprentices, Interns, Secondees-out, Secondees-In, Board Members, Non-Executive Directors, Contractors, Temps and Professional Services.
End User Computing (EUC)	EUC solutions refer to a range of tools adopted by individual data users to acquire, process and conduct analysis on data. Typically, in the format of excel files, access databases or Power BI reports (not limited to the list). An EUC is regarded as a sub-type of application.

Version control

Version Date	Author	Description	Approved by	Date approved	Date published
11/06/2021		First draft			
15/09/2021	[redacted]	Revised Section 7. Definition of terms to be consistent with 'the Policy'			
22/10/2021	[redacted]	Version 1.0 Final Approved by BBB Board on 22 October 2021	BBB Board	22/10/2021	11/11/2021
17/12/2021	[redacted]	Enhancements to security and standards			
22/02/2023	[redacted]	Version 2.0 DRAFT for PRG Annual Policy Review			

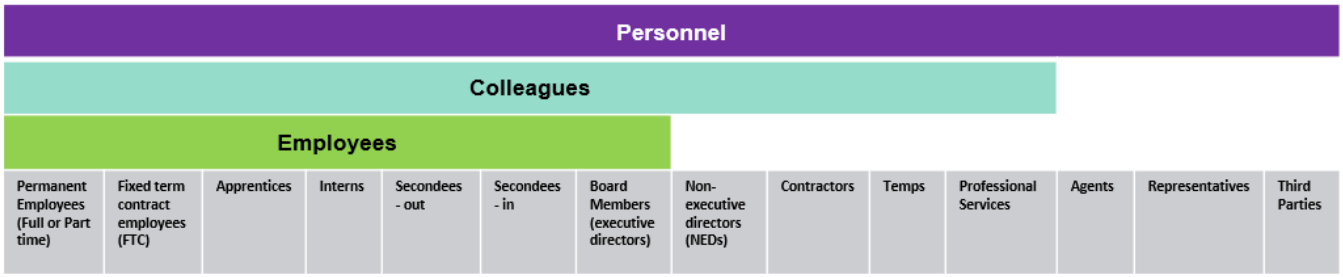
Appendix 1 - Policy Scope Categories

Accurate policy scoping is important to ensure that those who might be affected by a policy are identified and considered.

The proposed approach is to capture all potential individuals and entities that could fall within scope of a BBB policy into 3 distinct categories:

- Personnel
- Colleagues
- Employees

Policy owners will be responsible for identifying which category is applicable to their policy.



The Policy Governance Framework will capture the detailed list of which individuals fall within each category for reference. (Slide 3).

Policy Scope wording:

This policy applies to all BBB entities, operations and **Personnel**.

This policy applies to all BBB entities, operations and **Colleagues**.

This policy applies to all BBB entities, operations and **Employees**.