Data and Records Management Risk Policy

INTERNAL ONLY

Governance	
In support of the following Principal Risk Framework	Enterprise Risk Management Framework Operational and Resilience Risk Management Framework
Principal Risk	Operational and Resilience Risk
Sub Risk Type	Data and Records Management Risk
Approval date	26 August 2021
Last review date	1 September 2021
Next review date	30 September 2023
Location	Policy Hub

Ownership	
Accountable Executive (Group CRO)	Deon Raju Designation: Group Chief Risk Officer
Principal Risk Officer	Dawn Mthombeni Designation: Resilience Risk -Principal Risk Officer
Sub Risk type Owner	Not Applicable
Policy Owner (PRO or delegated official)	Dawn Mthombeni Designation: Resilience Risk -Principal Risk Officer
Policy Approver **Only to be completed where the Approver is different to the Policy owner or where a policy requires board or committee approval**	Dawn Mthombeni Designation: Resilience Risk -Principal Risk Officer
Policy Custodian (Contact)	Marius Marais Designation: Head-Governance, Policy and Regulatory Management

TABLE OF CONTENTS

Data and Records Management Risk Policy

1. POLICY CONTEXT

1.1 Introduction

The Data and Records Management Risk Policy, hereafter referred to as 'the Policy', specifies control requirements that must be read in conjunction with the Resilience Risk Management Framework (RRMF). It further sets out requirements relating to the way Absa Group business manage **Data** and **Records** in compliance with legal, regulatory and business requirements. Failure to execute appropriate controls to create/collect, process, protect, maintain or manage our **Data and Records** could result in material reputational, financial, legal or regulatory impact to the Absa Group.

This Policy is in support of the Enterprise Risk Management Framework and should be read in conjunction with any document listed in Section 4.1 'Related documentation supporting this Policy'.

1.2 Purpose

The primary objectives of the Policy are to:

- Provide an overview highlighting the key requirements to support Absa's Strategy regarding Data and Records Management.
- Provide the context, concepts, and definitions related to Data, Information and Records Management.
- Provide the Data Management Control Objectives.
- Provide the Records Management Control Objectives.
- Provide the minimum requirements applicable to Education and Awareness training.

1.3 Scope

1.3.1 In Scope

This policy applies to:

a. Absa Group Limited and all its subsidiaries (including any consolidated entity acquired via a debt-for-equity swap or created through a joint venture); and

b. All employees and workers of any entity within paragraph above; for the purposes of this document, "employees" includes permanent employees and fixed term employees; "workers" includes contingency workers (also referred to as agency workers) and secondees to Absa Group from a third party, irrespective of their location, function, and grade or standing. (Consultants and managed services workers engaged under a master services agreement with a third party is not in scope for this policy as the Data Control Obligations will apply. The only exception is if a consultant is seconded to Absa Group).

1.3.2 Out of Scope

This policy does not apply to:

- Any entity in which Absa Group Limited has any interest and which is a non-consolidated entity, or to any employee of any such entity; or
- Any entity which has been consolidated for International Financial Reporting Standards (IFRS) accounting purposes, provided Absa Group Limited has neither legal nor operational control.
  - By agreement between the Policy Owner and the Absa Group Limited Accountable Executive / Relationship Manager for a non-consolidated entity, specific control requirements incorporated within this Policy may be applied to the non-consolidated entity. In such cases, obtaining the agreement of the non-consolidated entity concerned or its other owner(s) to the control requirement(s) and the monitoring / oversight of the effective operation of the related controls, will be the responsibility of the relevant Accountable Executive / Relationship Manager."
  - *Such entities are likely to be special purpose vehicles (SPV) with a related* Absa Group Limited *loan which is in default and where* Absa Group Limited *has current and unilateral enforcement rights but does not have legal ownership / control.*

2. POLICY PROVISIONS / CONTROL REQUIREMENTS

2.1 Overview

- Absa needs to achieve its strategy in terms of: Treating all aspects of data as an asset which is useable and monetizable, though always within the boundaries of our ethics, prevailing laws and regulation.
- Meeting our customer and regulatory obligations.
- Ensure that the treatment of types of data and records are appropriate to the business purposes for which that data is captured, processed and retained.
- Draw an appropriate balance between value achieved from **Data, Information and Records management** activities and the cost of performing such activities.
- Given that the relevance and criticality of data varies across the organisation and cost and complexity increases with the level of rigour in data governance, to explicitly to avoid painting all data with the same brush, and instead accommodate different levels of rigour as appropriate to the data and any risks pertaining thereto.
- More modern risk and good-governance frameworks in South Africa view risk as the effect of uncertainly on an organisation's strategy and objectives. Therefore, it is essential that this Policy delivers effective risk management by supporting our business strategy.

In order to accomplish this, the Policy must align to the following principles:

- Defines **data, information and records**, their associated management disciplines and related concepts to ensure consistent application of this Policy and its accompanying Architecture Standard.
- Establishes **baseline** Data and Records Management objectives (i.e., the "what").
- Explicitly defines the applicability of these to different forms and classifications of data.
- To avoid friction, this Policy will explicitly not:
  - Introduce unnecessary layered governance and bureaucracy, instead removing it where appropriate.
  - Introduce unnecessary complex or adversarial control mechanisms or siloed, instead defining clear and collaborative mechanisms.
  - Introduce siloed control mechanisms or standards, instead defining a common and useable framework which can apply across the bank and across different aspects of data governance, management, risk and technology.
  - Introduce a non-implementable and impractical framework for Data and related disciplines in Absa.

The Risk Data Aggregation and Risk Reporting Policy (RDARR) Policy and related standards, specifies the minimum provisions and controls as per the requirements indicated under purpose to ensure transparency and accountability for RDARR. The policy stipulates requirements for the aggregation and reporting of risk data and associated governance and Information Technology (IT) infrastructure.

2.2 Context, Concepts and Definitions

In order to ensure consistent application of the Policy and Standard, it is necessary to outline several key basic concepts related to **Data, Information and Records management.**

A Cheat code supporting document has also been created to help and guide stakeholders across the organisation on how to implement and execute on key requirements.

2.2.1 Absa's Context and the Need for this Policy

As we move towards a more Digital Business Strategy, it is imperative that sound Data Management Principles should be adopted.

In a rapidly evolving, highly digital world there is limited utility in constructing very ornate data models for systems without the ability to use that data, either for analytics or, through integration, to make that data available for other purposes.

With increasing regulation, it is ever more necessary to understand data across multiple lines of business and multiple systems, ensure that that data is of sufficient quality to suit its intended purpose, service our customers appropriately and satisfy our regulatory obligations.

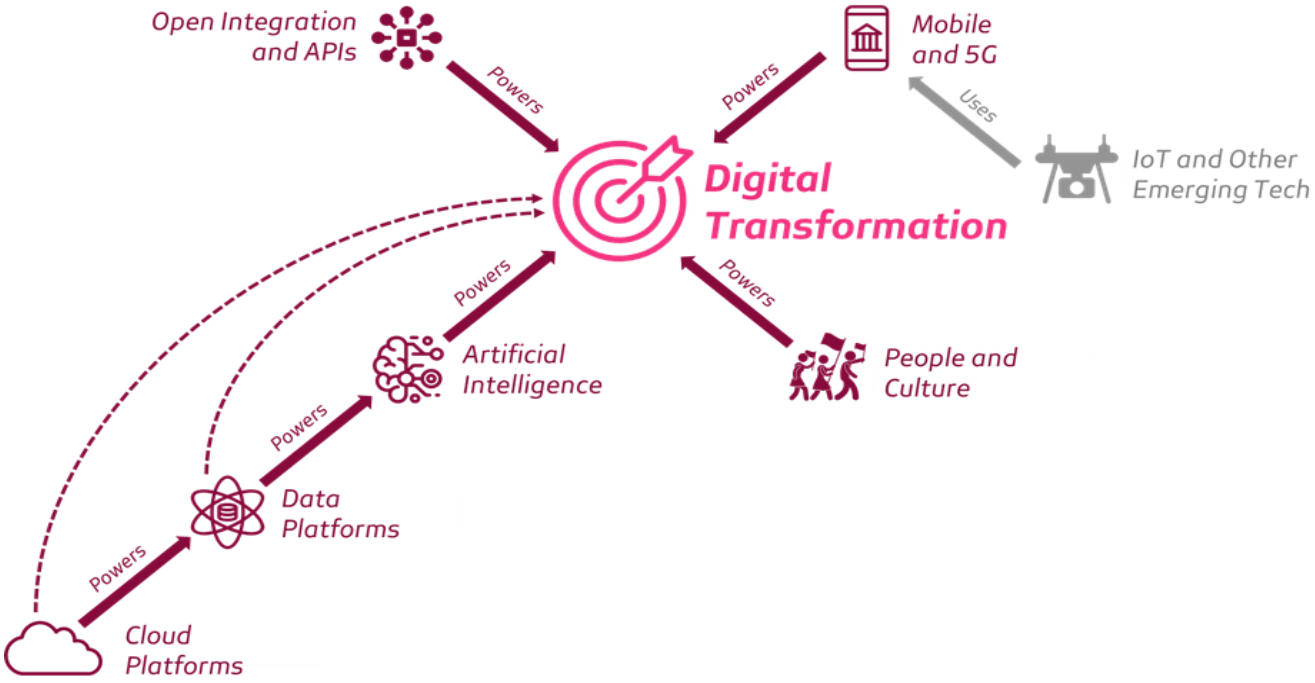
Furthermore, our customers' needs are increasingly left unsatisfied by subsets of functionality, manual workarounds and services which are not available in-the-moment.

Literature abounds online about the future of banking and emerging or potentially disruptive technologies attract their fair share of hype. Gartner highlights key "game changer" technologies as extracted from their survey of 379 Financial Services technology leaders.

Top performers highlight the following as the technologies most likely to move the needle:

1. Artificial Intelligence and Machine Learning
2. Data Analytics
3. Cloud
4. Digital Transformation
5. Mobile (Including 5G)

While we concur with these high-level observations, our own view is somewhat more nuanced. Rather than construe these independently or in isolation have come to see these things as parts of integrated approach. In our view, Digital Transformation is more of an end-goal that is gained through the integrated pursuit of these things together (and further, incorporating the aspects of Open Integration and APIs as well as the critical and foundational aspect of people and culture).



As a result of all of these factors, our approach to Data Governance and Management must support the selective use of these techniques as part of an integrated approach to Digital Transformation in line with our Strategy, rather than considering data in a silo under a non-integrated approach.

At the same time, all large incumbent financial organisations face increasing margin pressure due to commoditisation, competition and increased regulation- this means that we must reduce our costs as well as improve and differentiate our offering at the same time while having the capability to rapidly adopt to changing regulation without encumbering our progress towards our new offerings.

These things combined have given rise to our use of newer data management and governance techniques, newer technologies, and a departure from antiquated batch-based processing that happens several days (or even months) after the fact. It is noted, across the industry, that the Volume, Velocity, Variety and Veracity of data is increasing. In essence, our data disciplines are no longer constrained to slow moving batch processes, but must accommodate data which is constantly in motion, distributed across multiple businesses and systems and which is in a constant change.

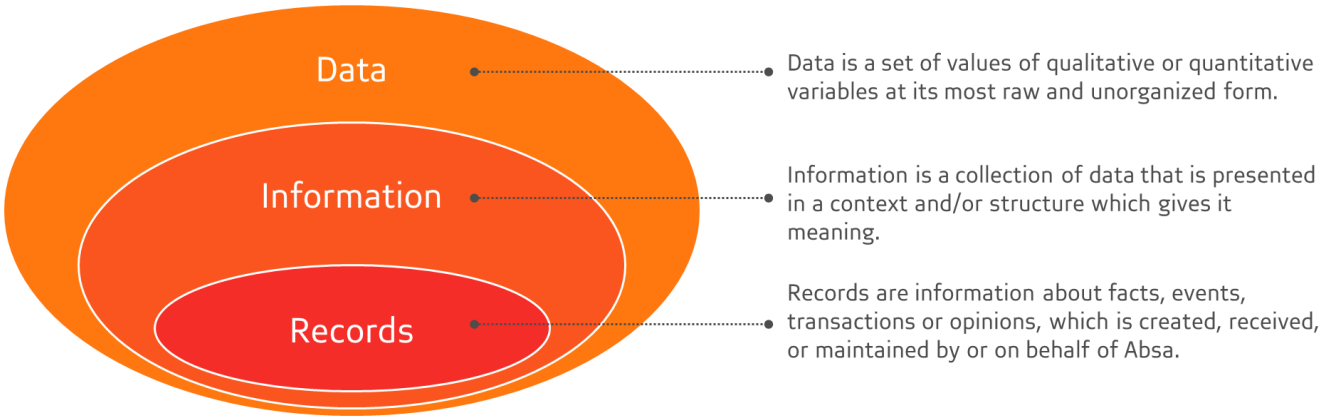
2.2.2 Language Used

Historically, we have observed confusion around what practices and controls are mandatory always, what should apply under certain circumstances or to certain kinds of data and what are merely recommendations. For this reason, we adopt a modified MoSCoW notation in this document.

Must	Must be in place to achieve success. This denotes a control or practice which is mandatory. If there are any conditions applying (e.g. applying to only certain kinds of data) then these are specified alongside.	Mandatory
Should	Should be in place, but success does not rely entirely upon it. Items identified in this way are often recommendations or constitute better ways to achieve the outcome. **Business Area/s** should apply critical thought and judgement on whether these make sense for them in the short or long term.	Recommended
Could	Could be put in place and would increase our degree of success. Very often this denotes optionality (e.g. several ways to satisfy a control requirement or objective), in which case the options are stated.	Suggested
Would	Would be put in place in future, but not required for immediate success.	Potential Future

2.2.3 Data, Information and Records

Although historically, these terms have often been used interchangeably, each has a clear and separate definition. At a high level, the diagram below, describes the relationship between the terms.



- **Data** is a set of values of qualitative or quantitative variables at its most raw and unorganised form. In general, data may exist inside electronic stores (like systems) or inside of physical stores (a filing cabinet). It may be structured (like SWIFT messages) or unstructured (free text or images). Raw data, is typically difficult to interpret, since it lacks context and meaning, e.g.:

  Translator, Johannesburg, Jabulani, 27, 11, 3157000, 2000, 91, Braamfontein, 1st Avenue, Cebekhulu

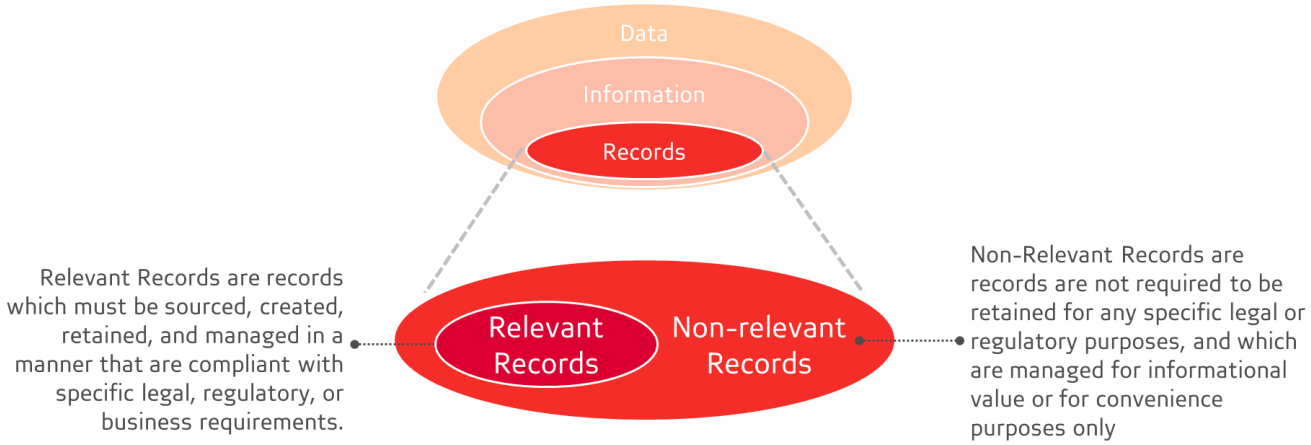
- **Information** is a collection of data that is presented in a context which gives it meaning, often making it more easily interpreted by machines or by human beings, e.g.:

Name: *Jabulani Cebekhulu*
Address: *91 1st Avenue, Braamfontein, Johannesburg, 2000*
Telephone: *+27 (0) 11 315 7000*
Occupation: *Translator*

- **Records** are **information** about facts, events, transactions or opinions, which is created, received, or maintained by or on behalf of Absa Group Limited (including those generated, processed or stored by third parties or customers) in carrying out its activities. In general, these are the information which are created and stored as a result of Absa's business dealings and activities, e.g.

If Absa were to provide Jabulani with a bank account, and the address above was provided as Jabulani's address for KYC purposes, it would constitute a record.

In addition, in order to accommodate different treatments for different types of records across our businesses, we separate records into two categories:



- **Relevant Records** are records which must be sourced, created, retained, and managed in a manner that are compliant with specific legal, regulatory, or business requirements.
- **Non-Relevant Records** are records which are not required to be retained for any specific legal or regulatory purposes, and which are managed for informational value or for convenience purposes only

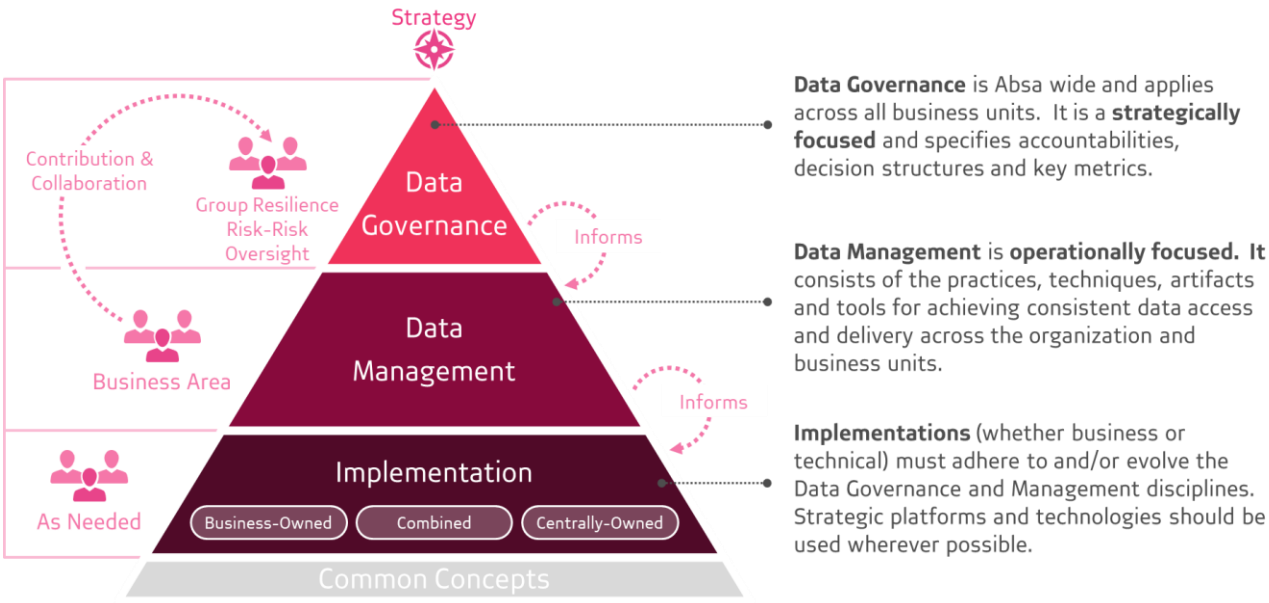
In the example above, Jabulani's address would constitute a relevant record, whereas the machine logs of Jabulani visiting our public marketing website would be a non-relevant record.

NB: *While the above distinctions are relevant, historically these have been pursued in silos leading to confusion and consternation. For this reason, and for simplicity we will use "**Data**" as the over-arching terminology going forward. In essence, we strive towards a more cohesive framework, which supports all the above.*

2.2.4 Data Governance and Management

Given Absa's strategy and operating model shift from Central Functions towards relatively autonomous customer focused Business Areas, it is necessary to develop newer, clearer, and more agile frameworks for the disciplines, which surround **data** and our **data** platforms. It is of critical importance that this framework is lean, avoids duplication and accommodates a gradient of rigour that can treat multiple forms and classifications of **data**.

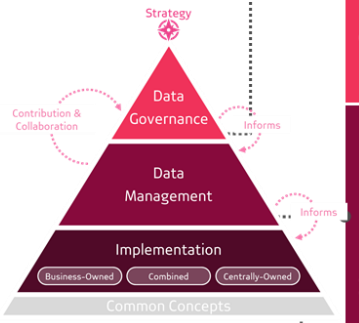
- A share point site has been created, named Cheat Codes whereby business areas can make reference to understand various technical components of Data Management and Architecture. It is a library of helpful information, contributed by experts across the organization.



- In order to balance Business Areas autonomy with scaled learning and re-use, there is a need to offer a separation of concerns between the responsibilities of business area and central teams. Thus, our definitions of **Data Governance** and **Data Management** will differ slightly from traditional definitions, as will our implementations thereof.

- **Data Governance** is the common set of capabilities that need to exist at group level for us to achieve our strategy. It is owned and curated at a central level but is built from collaboration with and contribution of all areas in Absa through a process of rigorous review and update (in the same way that "upstream contribution" takes place in the Open Source community).
- **Data Management** consists of the practices, architectural techniques, and tools for achieving consistent access to and delivery of data across the spectrum of **critical data** owners' areas and data structure types in Absa. This is a common framework informed by **Data G**overnance but falls to each business are to implement in a way which suits their needs as well as the needs of the businesses which are dependent upon them.
- **Implementations** refer to the actual day to day business or technology operations related to **data** and encompasses business processes, applications, technologies and integration. They are varied across the group and may be completely business-owned, completely centrally owned or under dual- ownership. Irrespective of the mode of ownership, they must both implement the applicable subset of Data Governance and Management practice to the degree that is appropriate and should err on the side of re-use of the strategic **data** platforms.
- **Common Concepts** enable effective collaboration and implementation across all the above (rather than unproductive or unnecessarily large meetings), it is necessary that the model is based upon common concepts. Where necessary these are defined within this document or will have their foundations in a **Common Ontology** or Semantic model to be described later.

The Key Responsibilities of each of the different teams involved for each layer of the model is expanded upon below and will be detailed in later sections:

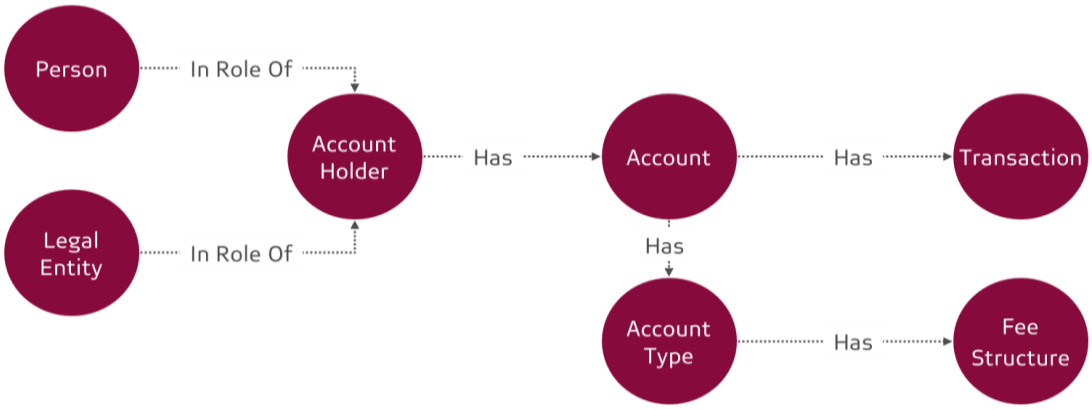


	Accountability	Key Artifacts and Activities		
Governance	Central Team	**Resilience Principal Risk Office** • Define and evolve policy and standard. • Aggregate KRI and metrics reporting across the group. • Conduct group-wide second line assurance functions. • Provide Sub-Risk Oversight over Data and Records Management Risk.	**CTO Data Engineering** • Implement core technical framework for central data platforms. • Review and contribute to Policy, Standards and group Architecture artifacts. • Evaluate tooling and automation options to support business.	**CTO Architecture** • Define group-wide architecture principles and practices. • Enable appropriate architecture practices and reviews are conducted across the group. • Support that data architecture receives due consideration across these reviews.
Management	Business Area	**Business Area Teams** • Ensure ownership by implementing data management structures and appointing data owners. • Identify critical data and other data of interest to them in their business (similar to BLOR) • Ensure data quality for data within their domain surfacing issues through the appropriate processes. • Ensure data matters receive due consideration when formulating strategy and roadmaps.		**Business Area Architecture** • Adhere and contribute to group architecture principles and practices. • Ensure appropriate architecture practices and reviews are conducted within the business unit, or elevated to the appropriate forum.,
Implementation	As Needed	**New Implementations (Projects)** • Abide by core change and architectural governance policies and standards. • Implement data management and measurement as part of the project scope.	**Existing Implementations (Live)** • Surface data issues through the appropriate processes. • Remediate issues and limitations either through BAU or projects, in line with business strategy and priority.	
		Mechanisms for doing this will be expanded upon in future updates of the relevant standards.		
Common Concepts				

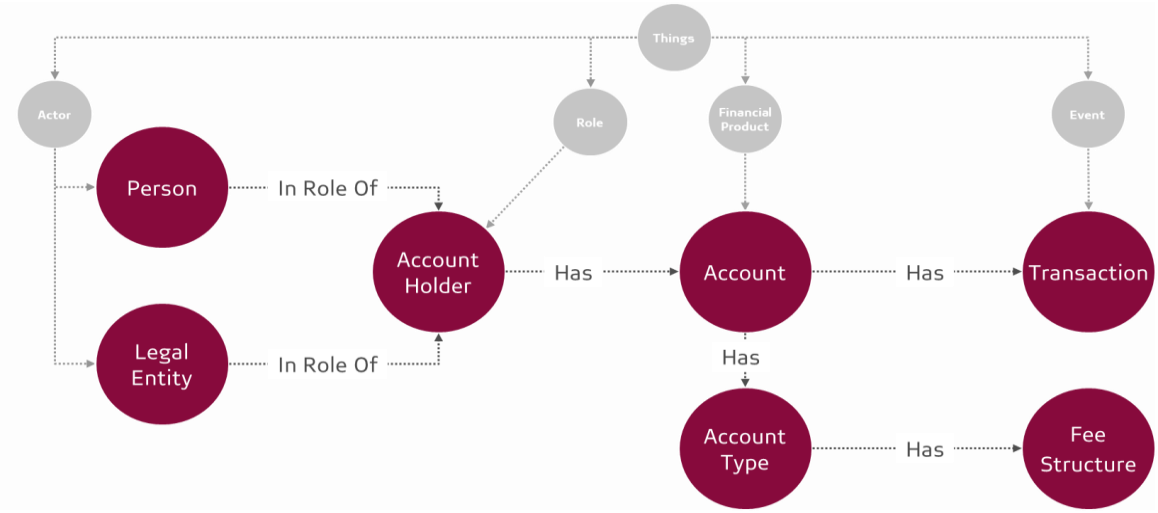
2.2.5 Organising and Modelling Data

In order to meet Absa's strategic ambitions with regards to data, it is necessary to define a framework which allows us to organise and manage our data appropriately. This section describes the key terminology used in that framework and in this Policy.

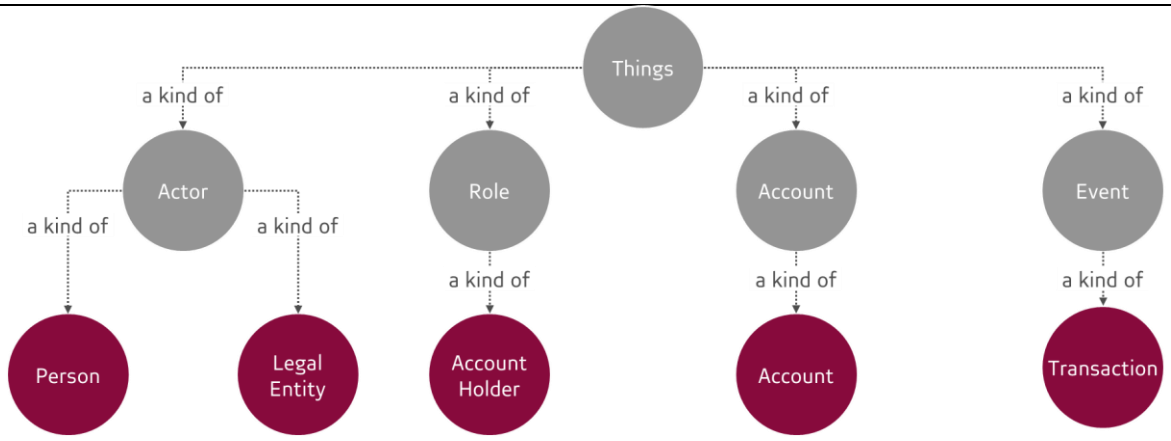
- An **Ontology** is a set of concepts (things) and the relationships between them that describes an area of subject matter. It typically contains formal naming and definition of these concepts, as well as the relationships between them and their categorization. Ontologies are typically used to organise knowledge about a particular subject or domain. They help to provide a clear basis for communication and can ease the burden of many activities (e.g. Integration, Data Governance). Various ontologies exist that describe banking and financial services e.g. Financial Industry Business **Ontology** (FIBO). An example of simple banking **ontology** is shown below. **Ontologies help us to communicate, reason, understand and infer.**



Ontologies typically use hierarchies or taxonomies within them to offer concepts of organization, inheritance and re-use. The **Taxonomy** above can also be absorbed into an **Ontology.**

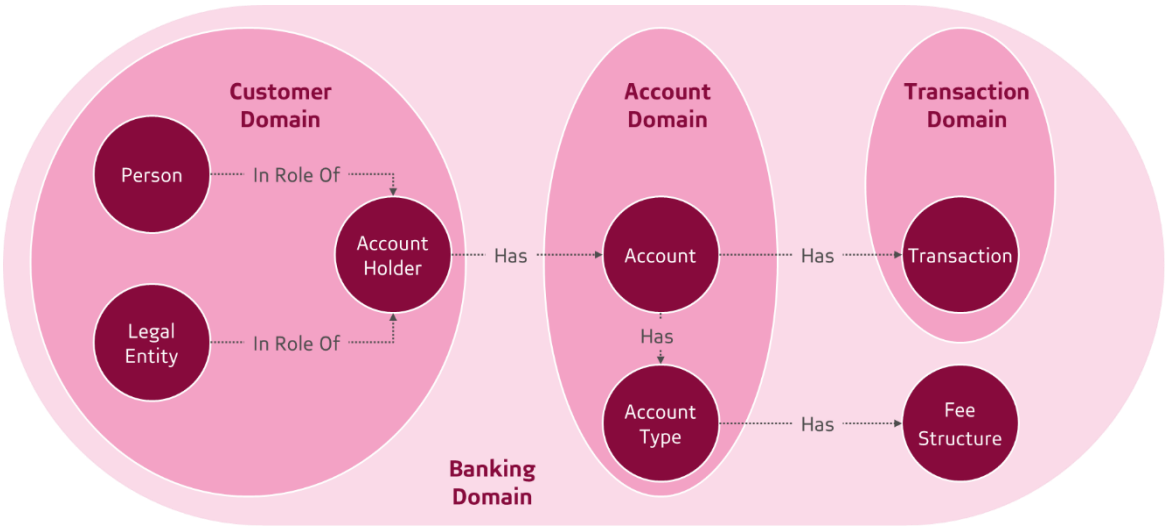


- A **Taxonomy** is a classification or categorisation of concepts (or things). It contains formal naming and definition of these but is generally limited to a hierarchy or grouping rather than describing all relationships between them. An example of a simple banking **taxonomy** is shown below. **Taxonomies help us to organise and locate things.**

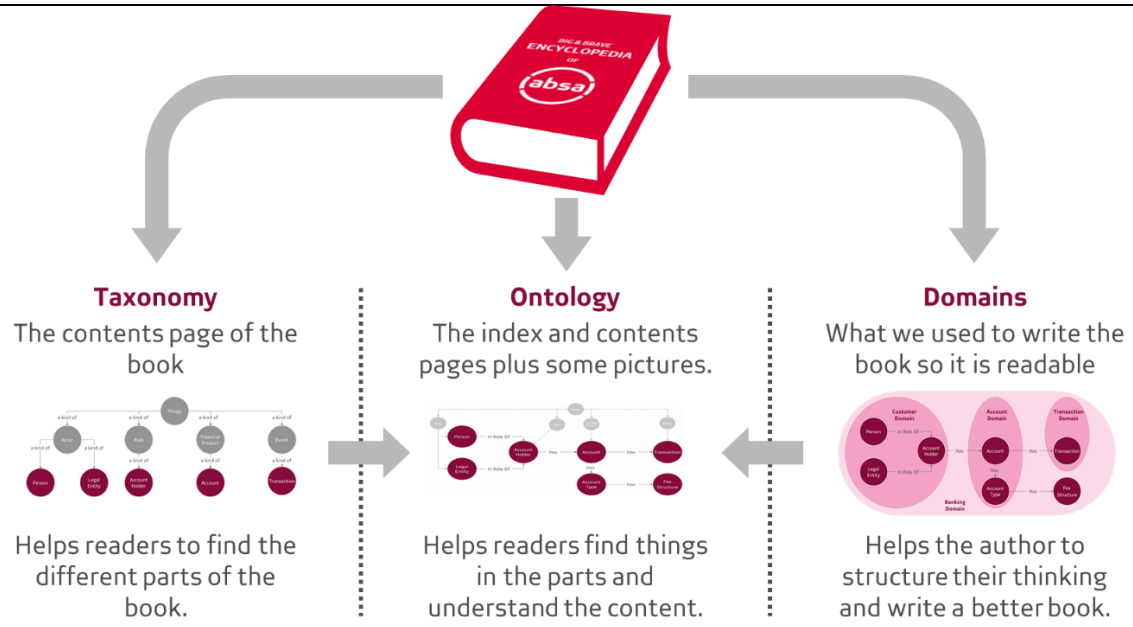


- A **Glossary** is a collection of definitions, typically collected for ease of reference purposes and typically organised alphabetically. However, in enterprise applications they have limited benefit since the meaning of a term typically varies depending on the context in which it is used (e.g. a "shoe" is very different if you are a "shoemaker" or a "horse rider").

- A **Domain** is a grouping of related concepts or subjects together, for convenience, design or implementation purposes. Architecturally, it often helps to group related concepts together since they may be dealt with by the same **business area** or in the same system. **Domains help us to communicate, reason, understand and infer, but more importantly to organize and build.**



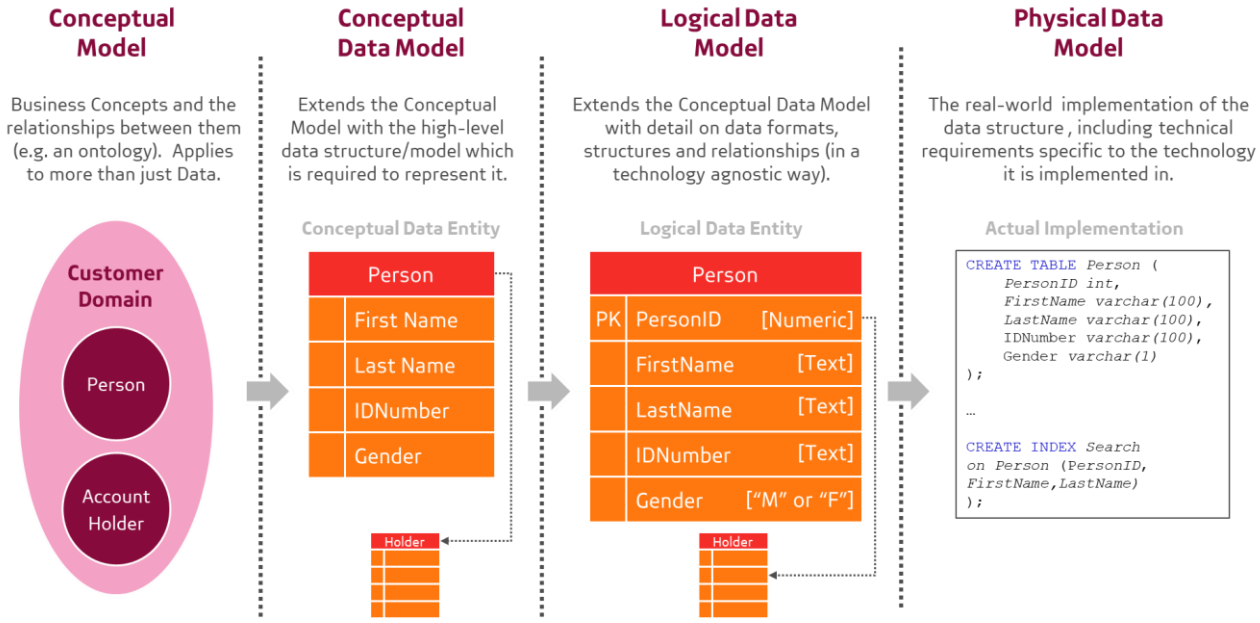
- A **Domains, Glossaries, Ontologies and Taxonomies all mechanisms for classification.** However, they fulfil different purposes for different audiences. The easiest way to understand this is to consider the example of writing a book about Absa.



NB: *Since Ontologies can embed the constructs of Taxonomies, Domains and Glossaries, going forward Absa will make use of a* ***domain-centric ontology-based mechanism*** *to organise its data. The* ***ontology*** *will be built out of the existing data inventories (such as Business Lists of Records) in a progressive way, which will be covered later. It is important to note that the current artefacts still have aspects of usefulness, but they will eventually be superseded by the new approach.*

The above is purely a conceptual and abstract representation of a simplified set of business relationships between concepts or things. For it to be practically useful, it is necessary to extend it to make it more concrete. The discipline of converting purely conceptual models like the one above into a practical and concrete implementation is referred to as **Data Modelling**.

Typically, different levels of data modelling are adopted for different purposes, different kinds of technology and applications. We will use the example of a subset of the Customer domain implemented in a traditional relational database to expand upon this.



- A **Conceptual Data Model** is a first pass of the data modelling process and be a summary or abstract-level model.
  - The abstract concepts of an organisation or subject area are translated into **Data Entities** at this level of modelling. Data entities are the objects or building blocks of the data model (e.g. the high-level data structure which represents a Person).
  - Data entities consist of **Data Elements** which are single pieces of **information** with a distinct definition (e.g. Last Name). These are sometimes also referred to as *fields* or *attributes* (especially in later stages of modelling)
  - Conceptual data models also reflect the high-level **Data Relationships** between entities along with business constraints as annotations (e.g. Account Holders must be a Person or a Legal Entity).

- A **Logical Data Model** describes the data of the Domain in as much detail as possible but excludes details around the physical implementation and is technology agnostic. Logical models contain entities in a more fleshed out form
  - Data Elements are expanded upon to contain their formats.
  - Relationships are reflected more precisely (e.g. through primary and foreign keys)
  - Many-to-many relationships are resolved in logical models and normalisation occurs.
  - Logical Data Models still use meaningful names (ideally business vocabulary from the conceptual model) to describe entities and attributes.
  - **Metadata** is "data about data" e.g. descriptions. **Business Metadata** is data that adds business context to other data. Logical data models typically include business metadata at the Data Element level where appropriate.

- A **Physical Data Model** is a representation of how a data model will be implemented using a specific technology, or the actual implementation represented through software artefacts like code (which is preferable in a DevOps context).
  - In a traditional relational database world, entities may be modelled as tables, attributes are modelled as columns, data types are specified according to the database technology.
  - Other technical considerations such as indexing, and partitioning can also be considered.

  NB: While the above represents conventional theory (derived from relational warehousing), the technologies and practices in use today require nuances and the above may be regarded as somewhat antiquated.

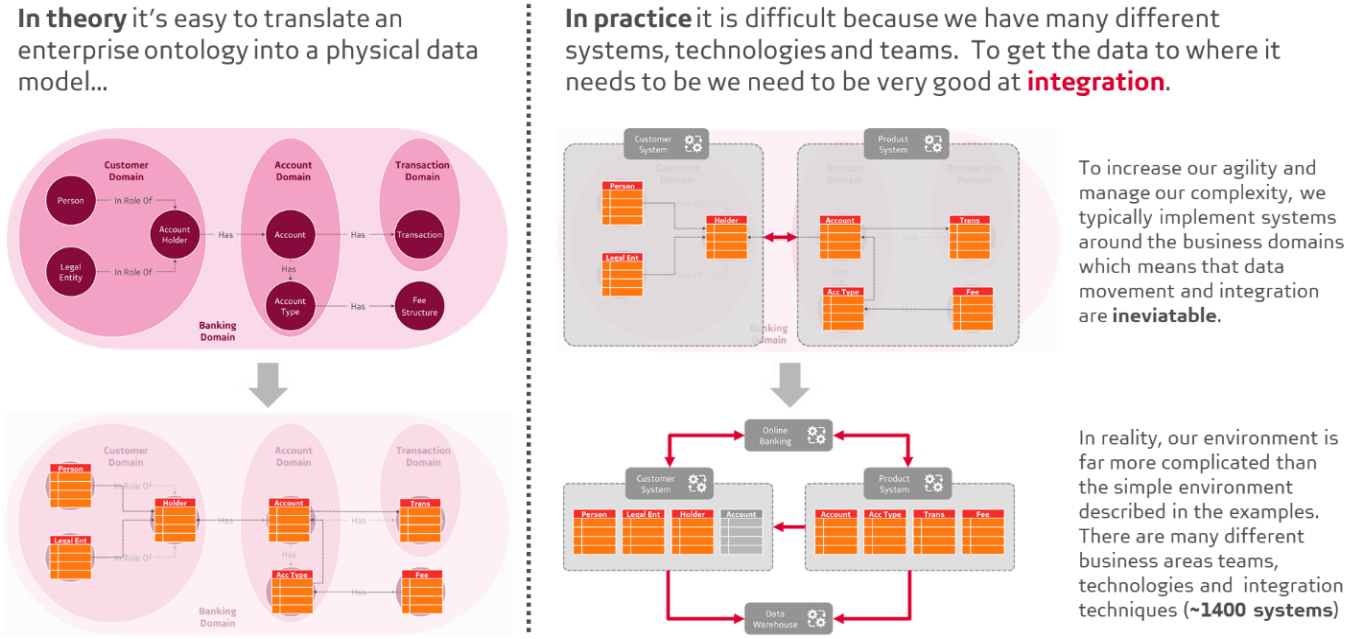
  Physical data models are highly dependent on the underlying technology and use case. This means that **logical data models must now take aspects of the target technology into account** as the model will vary significantly between different types of databases. A document-oriented database such as MongoDB will require a very different logical model than if a traditional relational database like PostgreSQL was used.

  With the **adoption of DevOps and Agile practices**, it is typical to condense the steps above into fewer steps with fewer static documentation artefacts being produced, instead striving towards self-documenting implementations. Nowadays, many modern applications only retain rudimentary elements of the data model inside the database itself and these are often implemented inside of application code. Therefore, none of the above conceptual explanation should be viewed as dictating mandatory deliverables and teams should, instead, exercise judgement in doing what is necessary, useful and fit for purpose.

  Data modelling, historically, was generally the domain of analytics and warehousing teams and was therefore very specific to data structures stored in a database. However, given today's highly integrated systems, open APIs and event driven messaging clear data representations are also key for **inter-system and inter-organizational communication**. Nowhere is this more apparent than the introduction of Open Banking and the rise of regulation such as PSD2 in the UK. This changes the way that data modelling processes are undertaken. Hence, in Absa, data architecture is not treated as separate from other disciplines within architecture, nor is it restricted to the realm of the "data warehouse".

Lastly, the implementation of physical data structures, while necessary, can also create a point of **change contention or delivery bottlenecks**. Data models are often implemented with a current purpose or set of needs in mind. Over time, as needs change, the data model or its physical implementation can become a bottleneck for change, both because it requires change and any application component referencing it may need to change as well (coupling). If these components are scattered across multiple systems or **Business Area/s,** that change becomes more complex and requires more energy to implement. If the database administration function is also separated from the application teams, it introduces an additional degree of complexity and friction. Teams are encouraged to think both about future change as well as data quality while implementing.

2.2.6 Data Manipulation and Integration



In order to manage the complexity of a large organisation and a high rate of change, we need to adopt certain key definitions and their associated management practices.

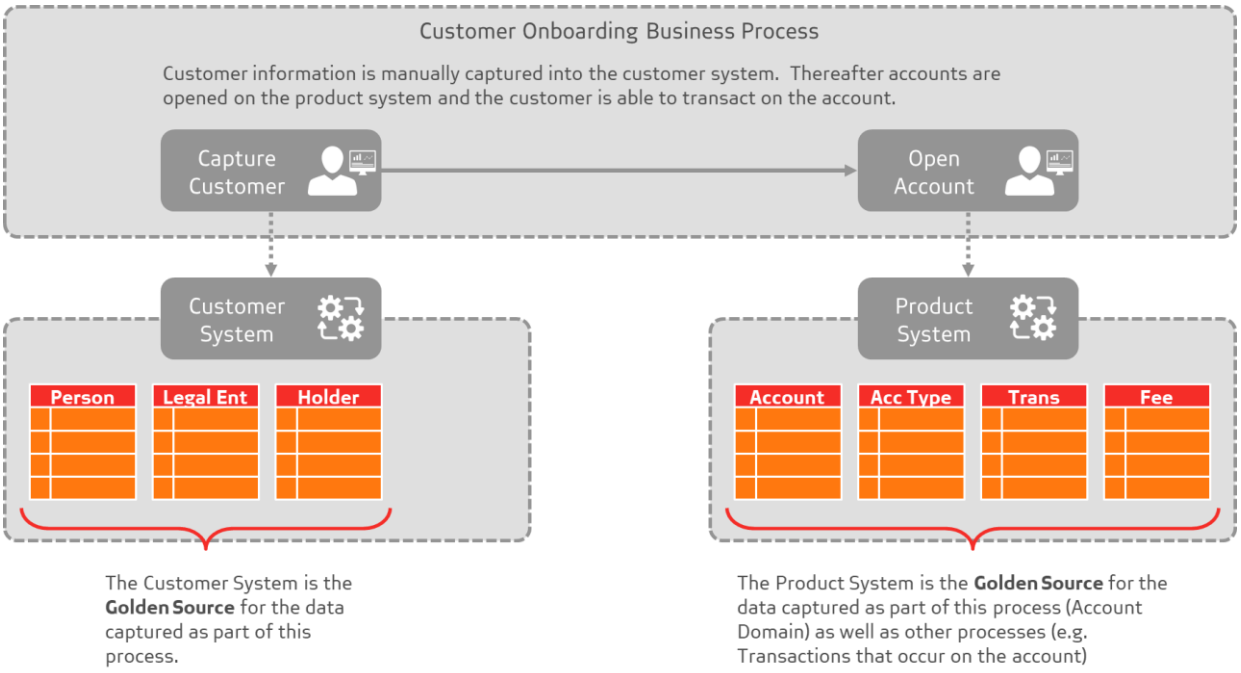
- **Data Lineage** is the life cycle of a piece of data, beginning with that data being created, how that data moves around the organization to reach its destinations, how it is transformed or manipulated in doing so and ultimately to where it is destroyed. These activities may take place whether by business process or by system activity. Data lineage exists so that we can understand where the data we use comes from and can make rapid decisions or changes over fast-moving data sets reliably. Data Owners should ensure that Data Lineage is mapped for all **Critical Data Elements/Entities.**
- **Data Integration** refers to the disciplines of moving data between systems and encompass Extract-transform-load type techniques or modern integration practices like real-time streaming and APIs. Sound data integration is an essential part of Data Lineage.
- A **Data Transformation is** the process of converting data from one format or representation to another.
- A **Source System** is any system or file that captures or holds data of interest. Data is extracted from a source system to send to target systems for further use. In integration terminology this may also be called a **Data Provider** or **Interface Provider**.
- A **Golden Data Source** is the system where data enters the organisation by being created, amended, generated through programmatic mechanisms or externally sourced.
- An **Authoritative Data Source** is a source of data that is established to be valid and a trusted source for a specific purpose or business requirement.
  - The controls, quality, ownership and authenticity of the content is considered highly reliable.
  - The system meets relevant engineering and architectural criteria and is a stable and desirable part of the enterprise environment.

- Ideally the bank should strive towards a single authoritative source for risk data per each type of data (in reference to BCBS principle 3 -accuracy and integrity: 36(d)). However, this may not always be possible given technical constraints, legacy implementations, geographic distribution or data sovereignty requirements or progressive migration activities.

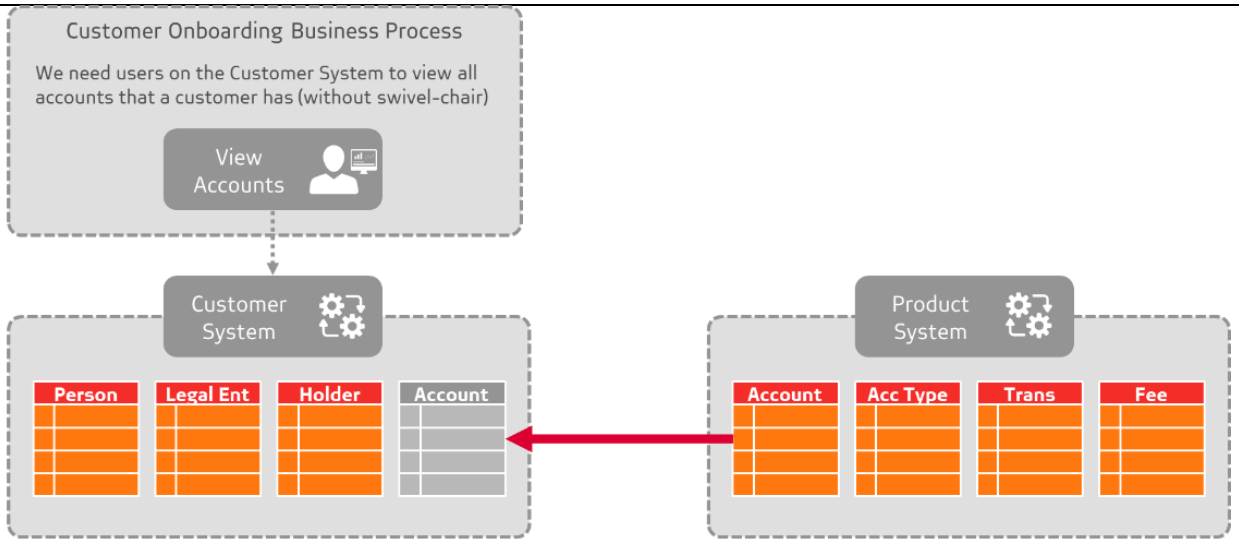
- A **Data Consumer** is a system or person that receives data for a specific use, which, in an ETL context may also be referred to as a Target System. It should be noted that ETL mechanisms are somewhat outdated and it is architecturally preferred to use other technologies such as APIs or streaming (which are real-time rather than batch oriented) where these are appropriate and feasible.

  These have caused confusion for many colleagues in the past and therefore we offer several examples to illustrate the concepts above following from our original domains and data models examples.

  - **Example 1 – Golden Source:** Consider a simple customer on boarding business process, where customer records are created in one system and accounts are created in another Product system, In the case of both systems they are indeed the **Golden Sources** for all the data they provide simply because the data is captured there and there alone. The lineage here is trivial given that it is created by a business process directly into the Golden Source.

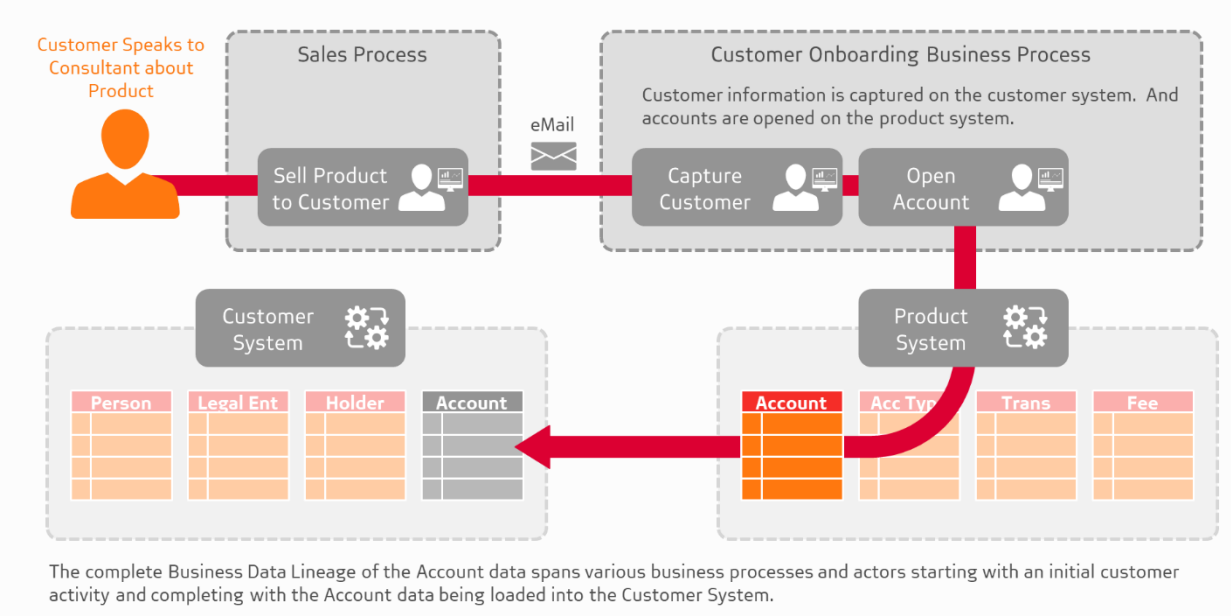


  - **Example 2 – Integration, Lineage and Authoritative Sources:** In a more complicated example we need to replicate the account **information** from the Product System to the Customer System so that the data can be viewed in a single place. We therefore have a copy of Account **information** stored within the customer system. We opt to accomplish this with a well-designed ETL Technology. This means that although the Customer System is not the Golden Source, it is still an authoritative source. The Lineage here is slightly more complicated since the data from one business process is moved around to serve a third need.



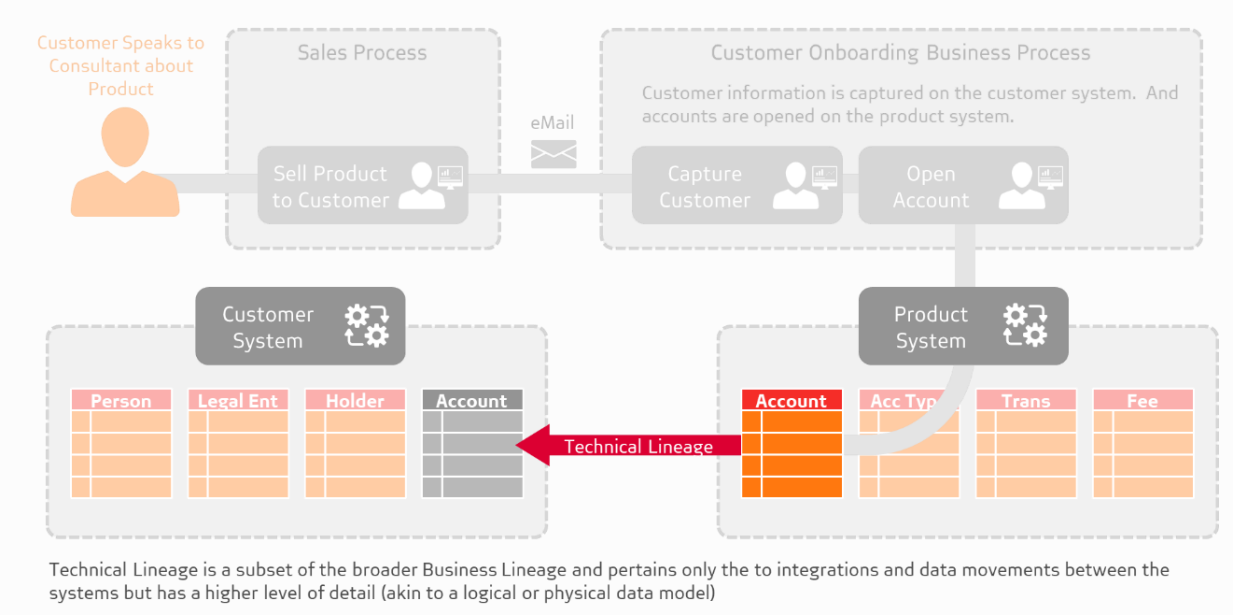
We do this by extracting all account data from the Product System and loading it into the Customer System (ETL). Because the data is faithfully and fully reproduced, though slightly manipulated the customer system is only the **Authoritative Source** for this data (not the Golden source)

Returning to the previous process example, the complete **Business Data Lineage** of the Account data spans various business processes and actors starting with an initial customer activity and completing with the Account data being loaded into the Customer System. The lineage of the Account data does not require all data in the source and target to be documented, merely the data which is moved. It is not always necessary or practical to document the full business lineage in this way.

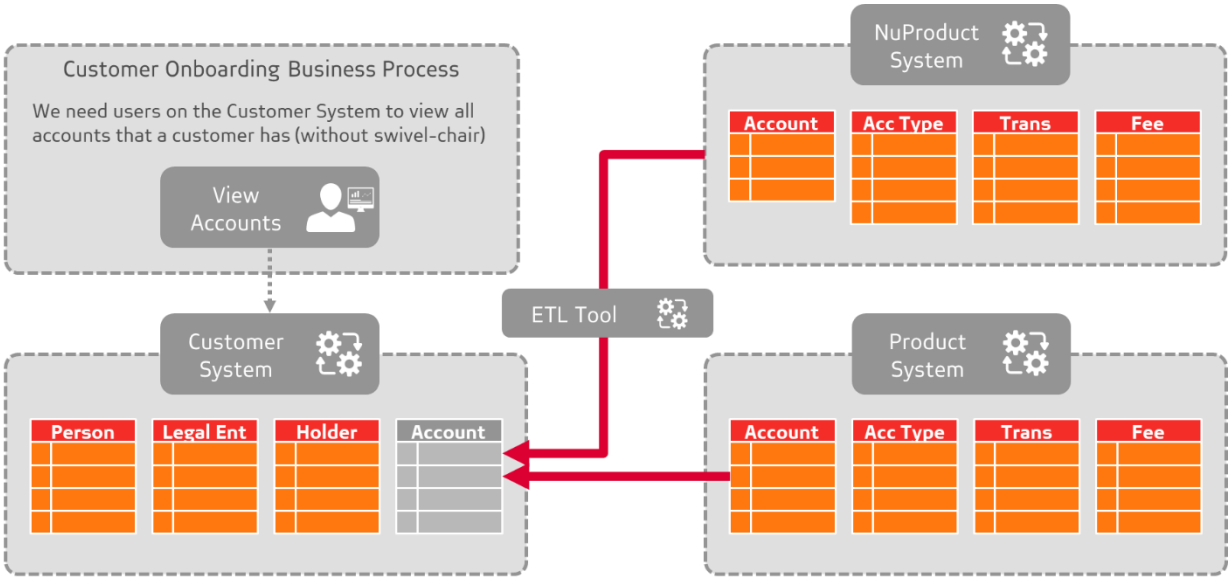


The complete Business Data Lineage of the Account data spans various business processes and actors starting with an initial customer activity and completing with the Account data being loaded into the Customer System.

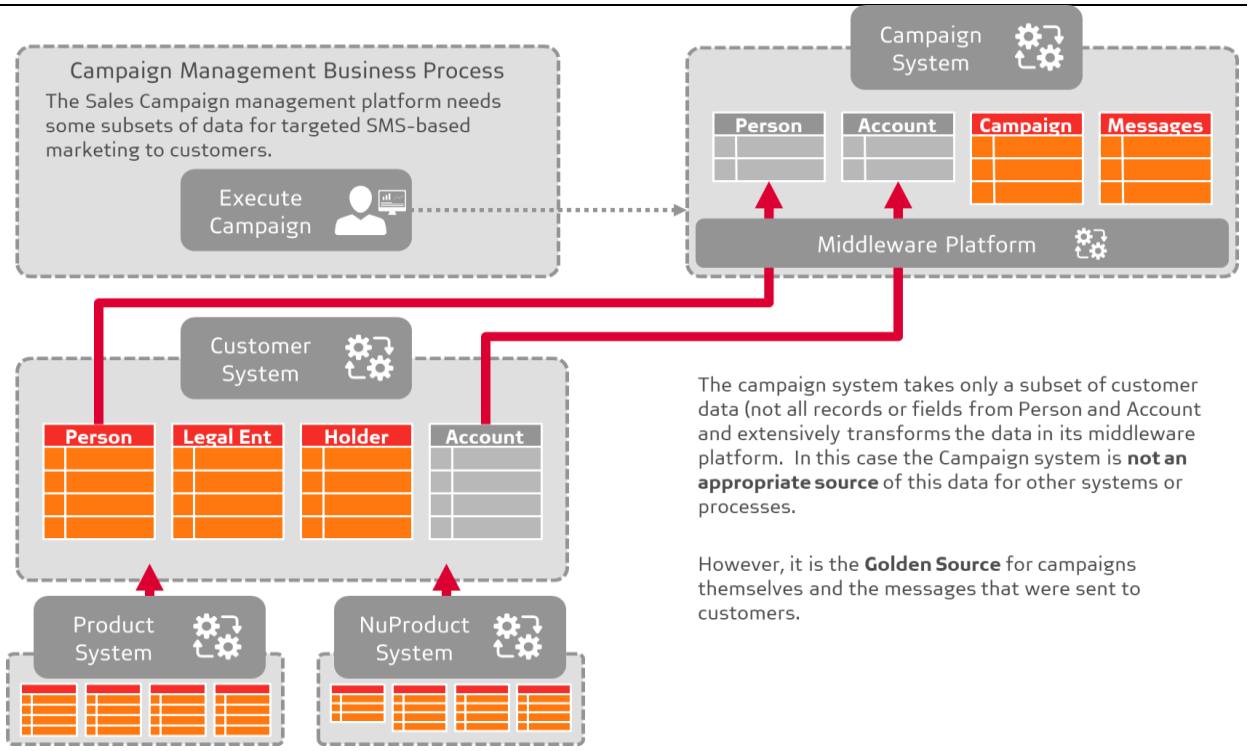
Technical Lineage is a subset of the broader **Business Lineage** and pertains only to the integrations and data movements between the systems but has a higher level of detail (akin to the difference between a conceptual and a logical data model). It is preferred that technical lineage be accomplished through self-documenting code and frameworks (such as spline), and not re-written in a separate artefact. The team (source system team, target system team or project team) performing the technical implementation will be responsible for ensuring that the **Technical lineage** is documented.



- **Example 3 – Leveraging Reuse:** Absa, however, is not a mono-product business and therefore does not have a single product system. In this example we consider the integration of a second product platform. If we introduce another product system (NuProduct) then it too can follow the same pattern so that all account **information** is available from a single Authoritative Source. Despite the introduction of an ETL tool, we under the Data Lineage and what transformations were done as part of the process. Since all data in the customer system is well understood, it remains an authoritative source and offers re-use and simplification by making all account data available in one place.

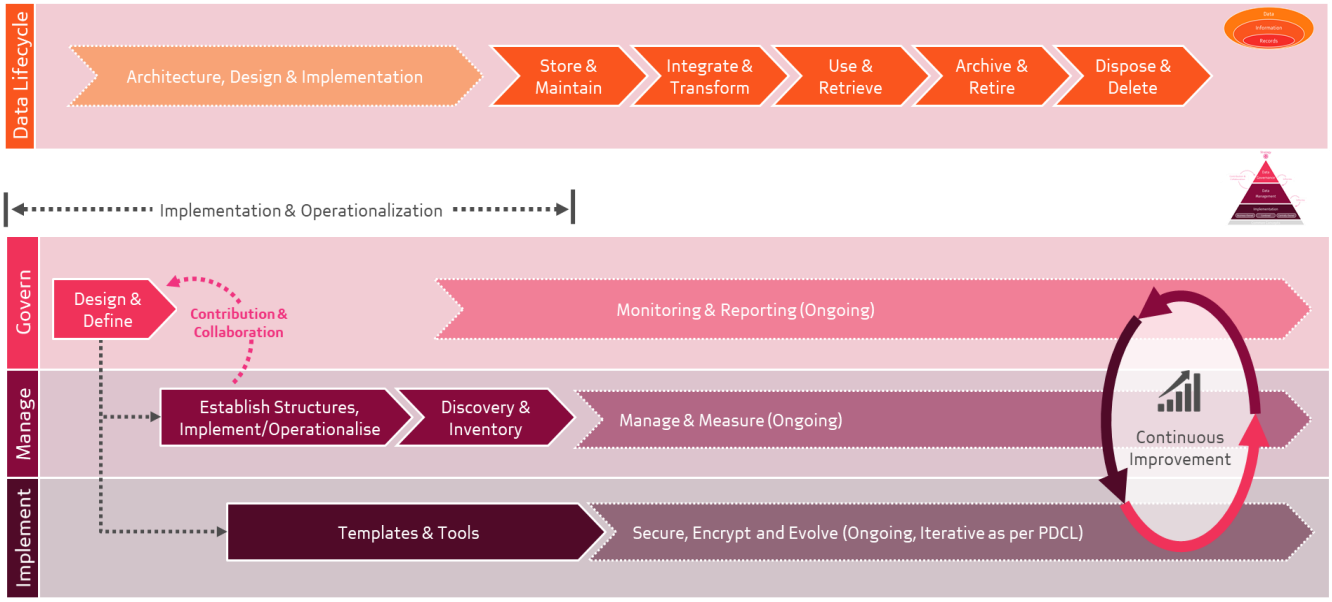


- **Example 4 – A Non-Authoritative Source:** Let us consider an example where circumstances make a data source non-authoritative. We introduce a new Campaign Management system, which uses proprietary middleware to consume only a subset of customer data (not all records or fields from Person and Account) and extensively transforms the data in its middleware platform. In this case the Campaign system is not an appropriate source of this data for other systems or processes. This would be doubly true if the transformations were not appropriately documented or self-documenting. However, it is still the Golden Source for campaigns themselves and the messages that were sent to customers.



2.2.7 Data Governance and Management Operationalisation Approach

Given that the future desired framework is different from the historical framework and aims to address various current challenges, there will be a progressive period of operationalisation. Just as the Data Lifecycle has various phases, there are different phases to operationalisation of Data Governance and Management, some of which will require the implementation of processes and technical solutions.



- **Design and Define:** In this step, the new Data Policy will be implemented. This is undertaken through a focused, collaborative process with the different **Business Area/s**.

- **Establish Structures, implement and operationalise:** In this step, **Business Area/s** establish the Data Management structures and processes within their businesses as suits their strategy and operating model, pursuant to the controls identified in the later sections of this document. In doing so, **Business Area** teams should consider their Business Strategy and direction of travel. This is first and foremost a design activity and **Business Area/s** should make use of their existing Data Management teams, their Architecture teams as well as Central Teams to help facilitate the process and address any issues.
- **Discovery and Inventory:** In this phase the **Business Area** teams must construct a **Data Inventory** of the **critical data** as a minimum and should also include any non-critical data which is of strategic importance to the business. This exercise spans data, which is created within the business, created in other areas that the business depends upon, or which is provided to other areas. In addition, it is necessary to perform Discovery to uncover any foreseeable constraints that may become challenges later or may impede progress towards strategy:
  - Teams should conduct a staffing and skills gap analysis to discover what skills and capacity are currently available and plan to address any deficiencies in line with their appetite. Various training assets exist within the group that can be used to assist in this process.
  - Understand the extent of people change, training and communications to be undertaken as part of the implementation phase.
  - Process-centric teams should understand and highlight any inherent constraints present in their business operational architecture (e.g. records inaccessible or un-indexed)
  - Technical teams should understand and highlight any inherent constraints present in their technology architecture (e.g. legacy packaged applications which are poorly understood and out of support).
  - Overall change ability and maturity should be evaluated to determine any gaps which will prevent the Inventory and Metadata from remaining consistent over time as projects are deployed into the environment.

- **Implement & Classify:** In this step, the **Business Area** teams add additional metadata to their data inventory. This will include mandatory metadata which must be populated as well as optional metadata which should be populated (at the **Business Area's** discretion). **Business Area/s** should make use of existing assets to assist with this process (e.g. BRIARs, Voltron metadata collected for RDARR, etc.) and avoid duplication of effort. This activity should largely be a collection/consolidation of different existing metadata and inventory sources. This may be undertaken in tandem with the Data Inventory of the previous step. Further, in this step it is necessary to implement the management practices and begin operating in the necessary management structures.
- **Templates and Tools:** In parallel with this work, the central team will compile a set of templates and re-useable artefacts which can be used by the **Business Area/s**. These will eventually be replaced by a strategic tooling stack to avoid performing this process in Excel and to improve the speed of change and accuracy of metrics reporting.

2.3 Data Management Control Objectives

2.3.1 Business Ownership

2.3.1.1 Control Statement: Business Ownership

In order to ensure that the Policy is a strategic enabler and are implemented across all **Business Area/s** in support of their strategies, it is necessary that the **Business Area/s** themselves have ownership of their data. This means that the **business area** has a defined mechanism for governance and data management which satisfies their strategic needs as well as those of the other areas which are dependent upon their data. This encompasses:

- **Data Inventory:** An inventory of **Critical Data** elements /entities of data created within the **business area** and **critical data** consumed from other areas, including **critical data** that is provided to other **Business Area/s.**
- **Data Owner(s):** Defining clear operational data ownership and accountability for **critical data** with Data Owner(s) appointed for each business domain. The Data owner must be a senior, permanent staff member who can effect change within the business and set priority of work undertaken in line with the business strategy. Where appropriate, the Data Owner may appoint Data Stewards as their delegates who will have day-to-day operational responsibility over the data. The Data Owner's accountability extends across the **Data, Information** and **Records management** life cycle as well, defining what data is critical, ensuring that data quality is well defined and implemented in their area. In addition, they or their delegates serve as the key point of contact for operational issues with their data which are encountered in other areas.

- **Steering Mechanism:** Establishing a defined mechanism through which data and related activities receive steer and priority from their leadership team or executives as well as a mechanism for issues which span different areas to be discussed and solved. It is left to the discretion of the **business area** as to how to implement this as it is inherently dependent upon their strategy and operating model. Appropriate Steering and or forums may be separate newly convened forums, existing forums, handled at the Business Exco or a combination thereof. This needs to be clearly documented and needs to adhere to the minimum requirements set out in the policy.
- **Cohesion & Collaboration Mechanism:** Establish a defined mechanism for cohesion of data management across the different areas of their business. This working forum or equivalent acts as the first layer of escalation for operational data issues and its chair or delegate acts as a single point of contact to receive, triage and route operational data issues from any other area where ownership cannot be established. During operational and project decision-making this mechanism must also ensure that the needs of downstream **Business Area/s** are considered.
- **Access Management: The business area** team must work with the Absa Logical Access Management Team to ensure that access to data is maintained in line with applicable policies and standards. Actual data owners or delegates must approve and review access to their data (whether that data is stored in shared platforms or not).
- **Technical and Architectural Soundness:** For effectiveness **Business Area/s** must ensure that their Cohesion and mechanisms incorporate their Architecture and Technical teams and that the Steering Forum incorporate the CIOs and Technical Leadership roles.
- **Fail-safe:** If all else fails, and these structures are not established, or data is not identified within the inventory, then the creator of any data is the data owner by default. This applies whether data is captured, received from a third party or derived from the data of others. This position can only be altered through the duly convened mechanisms above.

NB: The RDARR policy imposes additional criteria for data within its scope. These criteria should be read in tandem with these criteria.

2.3.2 Metadata Management

2.3.2.1 Control Statement: Establish an Absa Group Limited Data Taxonomy

Controls must be implemented by **Business Area/s** to identify, activate and manage data domains, to identify data elements and to define and manage business, operation and technical metadata.

2.3.2.2 Control Requirements

- **Data Inventory:** Creating and maintaining an inventory of **Critical Data** elements/entities must be established for data created within the **business area**, **critical data** consumed from other areas and **critical data** which is provided to other areas should be included.
- **Separation of Ownership of Shared Data Stores:** Where a single data entity is shared across **Business Area/s**, business rules must be defined between the **Business Area/s** to appropriately partition ownership at a **record** level. These should ideally be defined inside of the systems themselves.
- **Clear Definition:** Each **Critical Data Domain** contained in the Absa Group Limited Data Ontologies **must** have a clear definition, as must every Entity have identified within that domain. These **should** be captured in a standard format (to be set by the central Data and Risk teams) and made available in an openly viewable mechanism (e.g. Confluence).
- **Business Maintenance of Metadata: Business Area/s** must add and maintain their own Domains and Entities to the **Ontology** as appropriate for their business.
- **Golden & Authoritative Data Sources:** Business must abide by approved Group Architecture Authoritative Data sources for **Critical Data Entities** and should avoid unnecessarily duplicating data. Golden or Authoritative Data Sources must be used for data consumption. **Business Area/s** must declare their Golden and Authoritative Data Sources via the Inventory process.
- **Unique Data Sources:** Business Area/s and Functions, may identify a data source that is unique to their business and is not deemed a Golden or an Authoritative Source. In such a case the Business Area/ Function must ensure that following control attributes are met:
  - The data it contains is reliable (trusted, error-free and available).
  - The data is accurate.

- The data meets all other specified data quality attributes defined by the business.
- Business Area/s must declare their Unique Data Sources through the Data inventory process.
- This **Unique Data Source** should be reviewed by their Business Area Architects and Architecture Council in line this policy and Architecture Standard.

2.3.3 Data Architecture

2.3.3.1 Control Statement: Define, Document and Embed Data Architecture Principles

Business Area/s must process, manage and maintain data according to the defined Architecture Standard.

- A share point has been created for Cheat Codes whereby business areas can make reference to understand Architecture Principles.

2.3.3.2 Control Requirements

- **Architecture Principles:** The Chief Architect within CTO, must define and document Architecture Principles (these principles will include Data Architecture as part of the broader Group architecture).
- **Architecture Framework:** The Chief Architect, CTO must define an architecture management framework through which the relevant **Business Area** architects review relevant solutions in line with this policy and the Architecture Principles. This forms part of both the Architecture Standard as well as the core architecture artefacts of the group.
- **Architectural Alignment:** All **Business Area/s** and Functions must abide by approved Architecture principles (including the Data Principles contained therein) as well as the architectural governance and approval processes. These **would** be embedded within PDLC over time; Abiding also means that they have a responsibility to contribute to and evolve these principles over time.

2.3.4 Data Integration

2.3.4.1 Control Statement

Controls must be implemented to effectively monitor the successful transfer of **critical data** between environments to ensure that the data remains fit for purpose**.**

2.3.4.2 Control Requirements

- **Implementation Requirements:** System owners must take reasonable steps to ensure that the data being transferred from source to target has been delivered without loss (integration completeness) and its original state (integration accuracy), without accidental or undesirable modification. This will be validated by ensuring that architecture reviews were conducted as well as the completion of technical testing of the implementation.
- **Preferred Mechanisms:** The preferred mechanisms used to accomplish this could be one of the following:
  - Using a managed data transfer or object storage technology that has inbuilt transfer completeness and detection and failure reporting
  - Using a control file issued by the source environment which contains hash totals and **record** counts which are used by the target environment to compare load results thereby ensuring integration completeness and integration accuracy.
  - Using an asynchronous reconciliation mechanism at the business or technology level.
  - Other methods deemed appropriate and suitably mitigates the risk could also be considered.

2.3.5 Data Quality

2.3.5.1 Control Statement

Controls must be implemented to effectively monitor and manage the quality of data to ensure that it is fit for purpose.

2.3.5.2 Control Requirements

- **Data Quality Rules:** In order to ensure Data Quality, the Data Owner or their delegate must define business, technical and operational rules that specify Data Quality requirements for Data Domains and Data Elements. These rules should be considered at design time and implemented within the relevant systems to offer a measure of data quality. Where integrations are undertaken these rules could be used to measure and monitor Data Quality downstream. These quality rules should ideally be implemented in all source systems as part of their design. Where it is a requirement or where it is architecturally warranted, these rules could be implemented in integrations or in downstream reporting platforms. It is the responsibility of the Data Owner(s) to ensure that appropriate judgement is exercised in doing so and they should leverage the expertise of their architecture teams as well as the Central Data Engineering team. Business Area's must determine the relevant data quality rules and thresholds, based on their risk appetite.
- **Issues and Limitations:** Each Business Area is responsible for documenting issues and limitations (unable to meet a reporting obligation). These must be raised in a way which is visible to consumers (they proactively notify their consumers of their issues). This should therefore follow the IT Incident Management processes (a special class of Incident is to be created in ServiceNow for this). For Risk Data Limitations, please refer to the RDARR policy. All system or application related incident should be logged onto SNoW in order for the issue to be resolved and tracked, however for logging of event or issue which are Major or Critical these should be logged onto the approved Operational Risk System.
- **All Major and Critical Data Quality Issues and Limitations:** Data Owners must ensure that these have been raised and prioritised for remediation in terms of the Operational Risk Management Issue Management Standard and criticality assessed in terms of the Risk and Issue Classification Standard
- **Prioritisation of Data Quality:** Data Owner(s) must exercise judgement to prioritise Data Quality measurements based on the criticality and importance they have to their business as well as their consumers. The management structures within the business should act as an oversight mechanism to make sure that this is applied appropriately in line with the business strategy and objectives.

Noting that **not all** Data Quality Attributes are applicable or useful for all types of data, the following standard quality attributes should be considered for relevance when implementing data quality and the appropriate rules implemented.

Dimension	Explanation
Accuracy	Accuracy is the degree to which the data correctly represents the "real-life" value it is intended to represent when captured. Data must be sufficiently accurate to avoid a material impact on business. The data items should conform to the business definition and rules relating to them,
Completeness	Completeness is the extent to which the expected attributes of data are present. All mandatory data items should be assigned a value. **Business Area/s** and Functions should identify as a minimum all key mandatory data item and ensure that all are populated from initial data capture through to their use in calculations, reporting, collections and retention.
Consistency	Consistency is the extent to which data with the same definition must have the same value wherever it is stored or displayed. The **Business Area/s** and Functions should be able to demonstrate that the data is the same throughout the end-to-end process from initial data capture through to its use in calculations, reporting, collections and retention.
Precision	Precision measures whether the expected / required formats are provided with sufficient exactness, e.g. if the number of decimal places are not the same when utilised for different purposes, the difference when calculating total amounts could be substantial.

Dimension	Explanation
Timeliness	Timeliness is the extent to which data is sufficiently up to date for the use at hand. An acceptable time should be defined for all key data.
Uniqueness	Uniqueness implies that no specific record or entity appears more than once in a dataset and each **record** has a unique identifier.
Validity	Validity measures the degree to which data conforms to defined business rules. Validity is not synonymous with accuracy, which means the values are the correct values. A value may be valid, but still be incorrect. For example, a customer date of first service can be a valid date (within the correct range) and yet not be an accurate date.
Though these are not classical data quality attributes, cyber and information security frameworks typically make use of other (related) attributes to understand the criticality of data to the organisation and therefore to infer what practices should be used when handling, working with or securing that data. Strictly speaking, the below are not data quality attributes, but they are related - hence this section strives to alleviate confusion when working with both standards. Information Security and Cyber Risk Policy	
Confidentiality	The Information is accessible only by authorised individuals. An asset's Confidentiality considers how important preventing general or unauthorised access to the asset is to the organisation.
Integrity	The accuracy and completeness of the Information is maintained (e.g. the Information is not modified or corrupted and is only altered as expected). **In a security framework, integrity may be regarded as a superset of the above Data Quality requirements.**
Availability	The Information is accessible and usable when required

2.3.6 Operational Level Agreements and Service Level Agreements

2.3.6.1 Control Statement: Appropriate OLAs and/or SLAs in place.

Operational Level Agreement and Service Level Agreements must be in place when required to ensure that all relevant data quality attributes are met by the responsible Business area/s service provider.

2.3.6.2 Control Requirement

- An Operational Level Agreement (OLA) should be in place between the Owners of each source and target system. The OLA should specify requirements and controls that are needed to measure whether the source is providing the data at the quality, frequency (including defined delivery time) and format that is needed for the target system. It must also include roles and responsibilities and escalation processes should errors be identified. This is a mandatory requirement for all critical data in scope of RDARR.
- A Service Level Agreement (SLA) for external data suppliers (SLA) must be in place according to the Absa Group Limited Group Procurement requirements.

2.3.7 Data Lineage

2.3.7.1 Control Statement: Establish and Implement Data Lineage Principles and Guidelines

- In order to ensure that Data Lineage is documented and maintained in a consistent manner, Data Lineage principles and guidelines must be established and maintained.
- Refer to Section 2.2.6 Data Manipulation and Integration of this policy for Data Lineage Principles and guidelines**.**

2.3.7.2 Control Requirement

- **Applicability of Lineage:** Processes, Systems and End-User Developed Applications (EUDA) are all subject to the principles and procedures defined in this document.
- **End-User Developed Applications:** Most notably, concepts of Data Architecture, Integration, Lineage and Quality apply equally to end-user developed applications (though their implementation may vary). It is the responsibility of the implementer of these applications to ensure that they are developed in line with the applicable standards and policies and to seek the relevant architecture and risk approvals.

- **Business Ownership of Lineage:** All **Business Area/s** and Functions are accountable to ensure that the established principles and guidelines are implemented in line with their strategic objectives.
- **Data Owners Accountability:** Are accountable to ensure that lineage is documented for critical data elements.

2.3.8 Enterprise Reference Data

2.3.8.1 Control Statement: Appropriate Management of Enterprise Reference Data

Controls must be implemented to manage Enterprise Reference Data appropriately for specific types of data domains.

2.3.8.2 Control Requirements

- **Reference Data Architecture:** To ensure that Reference Data is managed consistently, Chief Architect, CTO must ensure that a Group-wide architecture principle are defined and implemented (including principles pertaining to Reference Data).
- **Single Authoritative Reference Data Source:** To ensure that a single, accurate and up-to-date version of Enterprise Reference Data is utilized within the organization, a single Reference Data source, which can be accessed by all consumers of such data, should exist.
- **Business Ownership of Reference Data:** Data Owner(s) must define each Reference Data Set that they own within their Data Inventory. **Business Area/s** must designate a single preferred, Authoritative Data Source for each Enterprise Reference Data set.

2.3.9 Data Migration

2.3.9.1 Control Statement: Clearly Defined Data Migration Approach

To manage business requirements and expectations for business-as-usual projects / change projects where data migration is in scope, the data migration plan must be clearly defined, documented and signed-off.

2.3.9.2 Control Requirements

- **Data Migration Lead:** Where applicable, projects must designate a Data Migration Lead who must define and document the scope for the data migration project to cover at minimum:
  - Whether data migration is required and is the most appropriate way to accomplish migration.
  - The in-scope source systems and / or applications.
  - The in-scope data sets that requires migration.
  - The in-scope Data Domains associated with the data sets that requires migration.
  - Any data sets that are specifically not in scope.
  - Technical considerations for accomplishing the migration
  - Confirmation from Business Owner and all relevant stakeholders that data was successfully migrated, and users tested applicable data quality attributes.
  - User tests and evidence of testing must be documented.

- **Data Migration Architecture:** The Migration Lead must obtain sign-off on the migration scope from the relevant architecture council (as part of the normal architecture review process for the project) as well as involved Data Owners of in-scope Data Domains and the project sponsor. It is noted that Data Migration is not always required within a project, and often, where it is required, such activities are more easily accomplished by adopting a co-existence architecture or strangler pattern.

2.3.10 Authoritative Data Sources

2.3.10.1 Control Statement: Establish a Process to Manage and Reuse Authoritative Data Sources

To allow Absa to achieve its strategy we need to ensure an appropriate degree of re-use within our data architecture. This is also required to comply with regulatory requirements i.e., RDARR requirements. Therefore, Absa **must** create and maintain a list of trusted Authoritative Data sources.

2.3.10.2 Control Requirement

- **Clear Review Process:** Business units and functions may propose data sources as authoritative for a data domain and/or business area scope via the inventory process.
- **Clear and Open List:** The list of authoritative data sources will be published in an open and accessible format for teams to access and discover the most appropriate data source to consume for a use case.
- **Authoritative Source Criteria:** Authoritative Data Sources must satisfy the controls outlined in this document as well as the architecture principles and must pass review with the appropriate architecture council. Most notably, for a source to be considered authoritative, it should abide by the following control requirements in this policy:
  - Business Ownership
  - Metadata Management
  - Data Integration
  - Data Quality
  - Operational Level Agreements and Service Level Agreements
  - Data Lineage
- **Usage:** When consuming data from any system, teams must make use of the authoritative source(s) as far as possible. Where not possible, the rationale and implication for not using an authoritative source should be reflected in the architecture strawman/blueprint and is subject to review and sign-off by the relevant architecture council.
- **If all else fails:** If only one data source for a data entity or domain exists and meets the above criteria, it is by default, the authoritative data source for that data. If data is landed into the core data platforms from an authoritative or golden source, in compliance to the above, then that data platform is considered authoritative for that data type (e.g. if Cheques Chassis Transaction data is landed into Hadoop in line with the above criteria, then Hadoop is an authoritative source for Cheques Chassis Transaction data). Only platforms deemed Core Data Platforms have this property. They can only be named by Chief Architect, CTO and must be ratified by the Group Architecture Council.

2.3.11 Data Jurisdictions:

2.3.11.1 Control Statement: Select Suitable Data Jurisdictions for Storing Data

With the advent of privacy legislation, the adoption of cloud technologies and the usage of third-party suppliers, Absa must ensure that data is stored in the appropriate jurisdictions (e.g. countries), in line with applicable laws, regulations, business risk, strategy and architecture. In intent, Absa may store data in any geography that satisfies our regulatory and risk requirements for a service with the noted exception of sanctions countries refer to the Sanctions Policy for details. However, decisions about which jurisdictions to adopt must take place through a structured process.

2.3.11.2 Control Requirement

- **Appropriate Assessment:** Assessing whether a provider or jurisdiction is appropriate requires deep judgement under a risk-based approach and the relevant approvals (which may include business risk acceptances, board approvals as well as the approvals of regulators themselves). Any team working with data, moving data across borders and utilising public cloud technologies should engage with the appropriate compliance, privacy, risk, engineering, architecture and security teams to ensure that they do so safely, that the correct assessments are undertaken, and the appropriate signoffs or risk acceptances are achieved. These are all incorporated within the Project Change Delivery Control Standard.
- While the above is the primary risk consideration we offer the following guidance that teams should follow:
  - Data may be stored outside of the country in which it is created only if this is done in a way which is compliant to regulation and law.
  - Where the above is possible, the time of writing it is a noted preference to host data in:
    - Ireland or Germany because of their suitable data privacy and regulatory environment as well as political stability,
    - In South Africa, either, inside of Absa's owned datacentres (private cloud) as well as public cloud infrastructure.
  - Given prevailing regulation and legal considerations, the other countries are preferred jurisdictions, except where the risk is acceptable to accomplish the business goal, or it is directly required in order to achieve this goal (e.g. the New York office stores data in the US to comply with regulation, some cloud provider services are not available outside of the US, etc.).
  - As per the Cloud Computing Policy various Cloud service models and deployment models exist. Any classification of data (Public, Internal, Confidential, Secret) may be stored in a cloud platform, irrespective of its deployment or service model, provided that the underlying cloud platform and provider satisfies Absa's control requirements, and any risks are understood, mitigated and risks accepted by the appropriate council.

2.4 Records Management Control Objectives

2.4.1 Identification, classification and indexing of records

2.4.1.1 Control Statement

An inventory of **Relevant Records** must be maintained

REF	Control Requirements	Physical	Electronic
a.	All **Relevant Records** must be classified according to the **Information** Labelling Schema as required by the Group **Information** and Cyber Security Policy.	✓	✓
b.	**Business Area** Accountable Executive must ensure that the **BRIAR** relevant to their business is reviewed and approved annually for accuracy and completeness or when a material change arises in a process or system.	✓	✓
c.	Relevant Records must be retained in accordance with the most recent applicable Country Retention Schedule(s). **Business Area/s** and Functions Accountable Executive must ensure the Retention Periods are applied to the Relevant Records reflected on the BRIAR.	✓	✓
d.	All **Business Area/s** and Functions must maintain an accurate and up to-date **Index of Records** to enable the identification and retrieval of records within the required timeframes defined in Section Retaining and storing of records.	✓	✓
e.	Records must be scanned through a process that adheres to applicable legal or local regulatory requirements for the capture of scanned documents. Scanning of records must meet minimum industry scanning requirements.	✓	✓

2.4.2 Retaining and storing of records

2.4.2.1 Control Statement

Legal and regulatory **record retention** requirements must be adhered to.

REF	Control Requirements	Physical	Electronic
a.	Applicable local legal and regulatory **records** management requirements must be identified and adhered to where these are more stringent than required by this Policy.	✓	✓
b.	**Records** must be retained in accordance with the most recent applicable **Country Retention Schedule(s).**	✓	✓

2.4.2.2 Control Statement

Records must be retrievable within required timescales.

REF	Control Requirements	Physical	Electronic
a.	**Electronic Records** must be retrievable within five (5) working days or within a period required by any applicable legal or statutory requirement; whichever is shorter.	N/a	✓
b.	**Physical Records** and archived **electronic records** that are not instantly accessible on a live system must be retrievable within 15 working days, or within a period required by any applicable legal or statutory requirements, whichever is shorter.	✓	✓
c.	**Record** Retrieval processes must be documented and tested at least every 12 months.	✓	✓

2.4.2.3 Control Statement

Records must be stored in a manner to protect the Integrity of the records.

REF	Control Requirements	Physical	Electronic
a.	**Records** must be stored in a manner which ensures they are protected from unauthorised access, and physical and environmental damage.	✓	✓
b.	**Business Area/s** and Functions must implement physical or / and logical access management controls as required by the Group **Information** and Cyber Security Policy and Group Physical Security policy to ensure **records** are restricted to only those employees who are appropriately authorised and need access to perform their duties.	✓	✓

2.4.3 Managing and protecting confidential records in use and transit

2.4.3.1 Control Statement

Classified records must be secured to maintain and protect their confidentiality, integrity and authenticity.

REF	Control Requirements	Physical	Electronic
a.	All employees (where applicable) must clear their workspace of **records** when leaving at the end of the day or for any other substantial period. **Records** must always be appropriately secured and protected - for example**, physical records** should be locked in a cabinet, drawers, or a safe when it is not being worked on. Computers should be locked physically and logically.	✓	✓
b.	All employees (where applicable) are accountable and responsible to protect records from inappropriate access when taken off-site. Where possible, employees should limit the number of records taken off-site.	✓	✓

REF	Control Requirements	Physical	Electronic
c.	Employees must not share **records** with any other person or employee that are not authorised to access the **record** nor share records through non-bank approved technologies or mechanisms suitable for that classification of record.	✓	✓

2.4.4 De-identification / Destruction of data and records

2.4.4.1 Control Statement

Records must be de-identified or destroyed in a timely manner upon expiry of their retention period.

REF	Control Requirements	Data	Physical	Electronic
a.	A process to identify **Data** and **records** required to be **destroyed** upon expiry of their **retention period** must exist.	✓	✓	✓
b.	**Data and records** must be securely **destroyed** within six months from **destruction** date. In a manner which does not support full or partial reconstruction / identification of the **record** when it has reached the retention expiry date or when the **record** is no longer required.	✓	✓	✓
c.	Contractual agreements must be in place with service providers to ensure secure **destruction** of **data** and **records**. Service providers must confirm in writing the details of records that are destroyed. Evidence of the authorisation and **destruction** of **data** and **records** must be maintained, using controls such as: • Physical certificates of **destruction**; and / or • **Electronic records** audit trail / reports of **data** and **records** deleted and / or • **Destruction** reports for storage media. (i.e. Hard Disks, cd's, microfiche);	✓	✓	✓

2.4.5 Disposal Hold

2.4.5.1 Control Statement

Disposal Hold of records must be adhered to.

REF	Control Requirements	Physical	Electronic
a.	**Business Area/s** and Functions must ensure, upon notification from Legal or Compliance, that any **records** subject to a **disposal hold** are suspended from **destruction** for the duration of the **disposal hold**.	✓	✓
b.	**Business Area/s** and Functions must ensure, upon notification from Legal / Compliance of a **Disposal Hold** being lifted, that all **records** impacted by the **Disposal Hold** have their applicable **retention period** reinstated. Where the **retention period** has expired, **destruction** must take place within three (3) months of the **Disposal Hold** being lifted (providing the **records** are not covered by another **Disposal Hold**).	✓	✓

2.5 Education and Awareness

In addition to mandatory training interventions, business representatives must provide ongoing awareness and socialisation to all employees handling data and records in their **business area** to ensure they are aware of their responsibilities to manage data and records responsibly and securely.

3. POLICY GOVERNANCE

3.1 Roles and responsibilities

Key roles and responsibilities to achieve the Policy requirements:

Level of Defence	Role	Responsibility
First line of defence - Responsible for the full suite of controls and associated content requirements related to evaluating, responding and monitoring business controls end-to-end.	Business Head / Accountable Executive 1st Line of Defence (1LOD)	• Accountable for the implementation of data and records management control requirements within their **Business Area.** • Responsible for setting up the operating model within their **Business Area** to drive compliance with this policy and associated standards.
	1st Line of Defence (1LOD)	• Manage data and records management incidents and must be logged onto an approved incident management system. • Responsible for driving compliance with this Policy and associated Standards. • Confirm that the Data and Records Management Policy and associated Standards are considered and implemented in Change initiatives, as applicable. • Report any non-compliance with the Data and Records Management Policy to the Business Line Manager on an on-going basis. • Confirm embedment of all operational Data and Records Management policy requirements for their **Business Area**. • Co-ordinate all operational Data and Records Management requirements within their respective **Business Area**.
	Data Owner	• Define clear operational data ownership and accountability for **critical data** with Data Owner(s) appointed for each business domain. • Appoint Data Stewards where applicable as delegates who will have day-to-day operational responsibility over the data. **Note:** • The Data owner must be a senior, permanent staff member who can effect change within the business and set priority of work undertaken in line with the business strategy. • The Data Owner's accountability extends across the **Data, Information and Records management** life cycle as well, defining what data is critical, ensuring that data quality is well defined and implemented in their area.
	Data Steward	Serve as the key point of contact where appointed by the data owner for operational issues with their data which are encountered in other areas
	System Owner	• Responsible to ensure that the system is operating efficiently and effectively, where data is captured, maintained, transformed, archived or deleted.

Level of Defence	Role	Responsibility
		• Take reasonable steps to ensure that the data being transferred from source to target has been delivered without loss (integration completeness) and its original state (integration accuracy), without accidental or undesirable modification. This will be validated by ensuring that architecture reviews were conducted as well as the completion of technical testing of the implementation.
	Business Area Architecture	Responsible to ensure that all new and amended solutions are approved by the relevant change and architecture councils and aligned to the Architecture Standard.
Second line of defence (2LoD) - Business Resilience Risk	Business Resilience Risk	• Confirm socialisation and/or training appropriate for the business. • Monitor and manage the Business risk profile in the context of approved risk appetite. • Escalate operational risk exposures in line with the RICM and ensure risks are correctly assessed. • Confirm that reporting requirements are adhered to. • Confirm that risk decisions are aligned with the requirements of the RICM and escalate as appropriate. • Identify, assess, monitor and manage all Sub Risks in business in line with the relevant policies & standards, supporting the PRO where required. • Perform an independent check and challenge of the Resilience Risk profile. • Perform assurance activity to ensure risk and control environment is operating effectively and deficiencies are identified and remediated which includes coverage over the sub risk. • Support the ExCo and check and challenge business and risk decisions where required. • Work with Resilience Risk PRO to define Business Area appetite and tolerance levels as well as the aggregated Group Level.
Second line of defence (2LoD) PRO Resilience Risk	PRO – Risk Oversight	• Implement an effective organisational design structure to manage the sub risk across the organisation. • Define requirements and cascade responsibilities accordingly within the group to ensure the sub risk is managed appropriately. • Implement an appropriate governance structure to enable monitoring and reporting. • Define a strategy to improve the proactive risk management of the sub risk. • Define and approve risk appetite and key risk indicators, aligned to the Group Risk Appetite Framework that are monitored on an ongoing basis and reported at least quarterly into the Absa Resilience Risk Governance structure. • Implement and embed the requirements of RRMF and its supporting polices and standards over their area of responsibility.

Level of Defence	Role	Responsibility
		• Define appropriate frameworks, polices and standards to manage the sub risk. • Review and approve dispensations, waivers and breaches against the sub risk policies and standards. • Develop and implement an effective combined assurance model for the sub risk. • Perform assurance activity against the RRMF, sub risk policies and standards to assess the design and operating effectiveness of the control environment ensuring deficiencies are identified and remediated. • Report on the sub risk with clearly defined key risk indicators and measurement criteria. • Escalate material risks and issues in accordance with the Risk and Issue Classification Matrix (RICM). • Support Resilience Risk to report significant risk type exposures and response plans to the Executive Risk Committee and Board Committees. • Operate as centres of excellence for the sub risk. • Monitor, review and challenge the effectiveness and adherence across the group to the RRMF, policies and Standards.
Third line of defence (3LoD) - Provides independent assurance and verification that the first and second lines are discharging their duties appropriately.	Absa Internal Audit	Perform independent audit on adherence to the Policy requirements.

3.2 Adherence

The provisions / control requirements of this policy are mandatory and are used to implement a group-wide approach for managing Data and Rec in support of the ERMF. Any deviations from these provisions / control requirements must be escalated per the requirements stipulated in Management of Dispensations, Waivers and Breaches Standard.

Non-adherence to any requirement in this policy may result in disciplinary action, which could lead to dismissal.

3.3 Principal Risk Impact

It is to be understood and expected that, in the execution of the requirements detailed in this standard, the frameworks, policies and standards of other Principal Risks – as detailed within the ERMF – may apply and interact invariably with the requirements set out in this standard and are to be complied with.

3.4 Reputational Impact

Any action or inaction taken relevant to this standard which may have the potential to incur reputation risk for Absa Group Limited, i.e. likely to result in material criticism and/or censure of Absa Group Limited by key stakeholders or opinion formers (including clients, market counterparties, regulators, government officials, law enforcement agencies, media or Non-Governmental Organisations (NGOs)) must be escalated to reputationrisk@absa.africa according to the Reputation Risk Framework.

3.5 Data Privacy

For all personal data that is collected, processed, stored, shared, archived or destroyed under this Standard, the control objectives and minimum control requirements of the Data Privacy Policy and Data Privacy Standard must be complied with.

3.6 The Absa Way Code of Ethics

The Absa Way Code of Ethics outlines our values and expected behaviours when engaging with our fellow employees, customers, clients, shareholders, governments, regulators, business partners, suppliers, competitors and the broader community. The behavioural standard set by the Absa Way applies to every Absa employee and colleague across our business globally. The objective is to define the way we think, work and act at Absa to ensure that we deliver against our Purpose of helping people to bring their possibilities to life.

Absa takes the Values and Behaviours and points set out in this Code of Ethics very seriously. It is every colleague's responsibility to be aware of, understand, and behave according to this Code of Ethics and the policies that apply to their roles. Any failure to act in accordance with the Values and Behaviours or any breach of this Code of Ethics may result in disciplinary action, up to and including dismissal.

4. REFERENCES

4.1 Related documentation supporting this Policy

The following documents must be referred to during the execution of this Policy:

- Enterprise Risk Management Framework
- Operational and Resilience Risk Management Framework
- Risk Data Aggregation and Risk Reporting Policy (RDARR)
- Risk Data Aggregation and Risk Reporting Limitations Standard
- Information Security and Cyber Risk Policy
- Technology Risk Policy
- Cloud Computing Policy
- End User Developed Applications (EUDA) Standard
- Physical Security Policy.
- Country Retention Schedules - Supporting Document
- Data Privacy Policy
- Fraud Risk Policy
- External Supplier Sourcing Standard
- External Supplier Management Standard
- Information Security and Cyber Risk Policy
- Product Delivery Lifecycle Standard
- Project Change Delivery Control Standard
- Architecture Standard

4.2 Glossary

This glossary provides acronyms and definitions that are specific to the content of this document:

4.2.1 Abbreviations / Acronyms / Terms

Abbreviation / Acronym / Term	Explanation
BA	Business Area
BRIAR	Business Records and Information Asset Register
CTO	Chief Technology Office

Abbreviation / Acronym / Term	Explanation
ERMF	Enterprise Risk Management Framework
ERMF	Enterprise Risk Management Framework
IAR	Information Asset Register
IFRS	Financial Reporting Standards
NGOs	Non-Governmental Organisations
OLA	Operational Level Agreement
RDARR	Risk Data Aggregation Risk Reporting
RICM	Risk Issue Classification Matrix
SCO's	Supplier Control Obligations
SLA	Service Level Agreement

4.2.2 Definitions

Definition	Explanation
Authoritative Data Source	A source of data that is established to be valid and a trusted source for a specific purpose or business requirement. • The controls, quality, ownership and authenticity of the content is considered highly reliable. • The system meets relevant engineering and architectural criteria and is a stable and desirable part of the enterprise environment. • Ideally the bank should strive towards a single authoritative source for risk data per each type of data (in reference to BCBS principle 3 -accuracy and integrity: 36(d)). However, this may not always be possible given technical constraints, legacy implementations, geographic distribution or data sovereignty requirements or progressive migration activities.
Business Area/s	All Business Area/s within Retail and Business Bank (RBB), Corporate and Investment Bank (CIB), Insurance Cluster, Absa Functions and Countries.
Conceptual Data Model	A first pass of the data modelling process and be a summary or abstract-level model.
Country Retention Schedule(s)	Centrally maintained schedule per country of the retention period(s) required for Legal and Regularity purposes.
Critical Data Element/Entities	Data/data elements/Entities that is vital to the success of the business area objectives and operations and if the data is compromised or not managed appropriately the business will be exposed to risks that could lead to financial losses, legal issues and the loss of licence to operate as a registered Financial Service Provider.
Data	A set of values of qualitative or quantitative variables at its most raw and unorganised form. In general, data may exist inside electronic stores (like systems) or inside of physical stores (a filing cabinet). It may be structured (like SWIFT messages) or unstructured (free text or images). Raw data, is typically difficult to interpret, since it lacks context and meaning,
Data Consumer	A system or person that receives data for a specific use, which, in an ETL context may also be referred to as a Target System. It should be noted that ETL mechanisms are somewhat outdated, and it is architecturally preferred to use other technologies such as APIs or streaming (which are real-time rather than batch oriented) where these are appropriate and feasible.

Definition	Explanation
Data Domain	A grouping of related concepts or subjects together, for convenience, design or implementation purposes. Architecturally, it often helps to group related concepts together since they may be dealt with by the same business area or in the same system. Domains help us to communicate, reason, understand and infer, but more importantly to organize and build.
Data Integration	The disciplines of moving data between systems and encompass Extract-transform-load type techniques or modern integration practices like real-time streaming and APIs. Sound data integration is an essential part of Data Lineage.
Data Lineage	The life cycle of a piece of data, beginning with that data being created, how that data moves around the organization to reach its destinations, how it is transformed or manipulated in doing so and ultimately to where it is destroyed. These activities may take place whether by business process or by system activity. Data lineage exists so that we can understand where the data we use comes from and can make rapid decisions or changes over fast-moving data sets reliably. Data Owners should ensure that Data Lineage is mapped for all **Critical Data Elements/Entities.**
Data Transformation	The process of converting data from one format or representation to another.
De-identify / De-identification	The process of deleting any data that: a. Identifies the data subject. b. Can be used or manipulated by a reasonably foreseeable method to identify the data subject. c. Can be linked by a reasonably foreseeable method to other data that identifies the data subject.
Destruction	**Destruction** of data / **record** no longer required / expired aligned to the **retention period** set out in the **Country Retention Schedules**.
Disposal Hold	Upon notification from Legal / Compliance, any records covered by a **Disposal Hold** are suspended from **destruction**.
Electronic Records	**Information** recorded in a manner that requires a computer or other electronic device to display, interpret, and process it.
Glossary	A collection of definitions typically collected for ease of reference purposes and typically organised alphabetically. However, in enterprise applications they have limited benefit since the meaning of a term typically varies depending on the context in which it is used (e.g. a “shoe” is very different if you are a “shoemaker” or a “horse rider”).
Golden Source	The system where data enters the organisation by being created, amended, generated through programmatic mechanisms or externally sourced.
Index of Records	An inventory of records stored.
Information	A collection of data that is presented in a context which gives it meaning, often making it more easily interpreted by machines or by human beings
Information Asset	This is **information** relevant to the operation of the bank. The asset can be in the form of a: a. Document, paper or digitized format b. Electronic **record** c. Voice recording d. Microfiche

Definition	Explanation
Logical Data Model	Describes the data of the Domain in as much detail as possible but excludes details around the physical implementation and is technology agnostic. Logical models contain entities in a more fleshed out form.
Non-Relevant Records	Records which are not required to be retained for any specific legal or regulatory purposes, and which is managed for informational value or for convenience purposes.
Ontology	A set of concepts (things) and the relationships between them that describes an area of subject matter. It typically contains formal naming and definition of these concepts, as well as the relationships between them and their categorization
Personal Data	Any data (including special personal data) relating to a living, natural person and where applicable, an existing juristic person, either in electronic or hard copy format, from which an individual or juristic person can be identified. This includes but is not limited to race, gender, sex, pregnancy, marital status, national, social or ethnic origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language, birth of person, education background and history, financial history, employment history, criminal history, email address, physical address, location **information**, mobile numbers, online identifiers (e.g. cookies or IP addresses), biometric **information**, an identifying number or symbol, the personal opinions, views or preferences of the person, the opinions of another individual about the person, the name of the person if it appears with other personal data relating to the person or if the disclosure of the name itself would reveal **information** about the person, correspondence sent by the person that is implicitly or explicitly of a private or confidential nature, or further correspondence that would reveal the contents of the original correspondence.
Physical Data Model	A representation of how a data model will be implemented using a specific technology, or the actual implementation represented through software artefacts like code (which is preferable in a DevOps context).
Physical Records	The original paper copy, printout, or any **record** that can be read without the use of a computer or other electronic device.
Qualitative data	Measures of 'types' and may be represented by a name, symbol, or a number code.
Quantitative data	Measures of values or counts and are expressed as numbers. **Quantitative data** are data about numeric variables (e.g. how many; how much; or how often).
Record	**Information** about facts, events, transactions or opinions, which is created, received, or maintained by or on behalf of Absa Group Limited (including those generated, processed or stored by third parties or customers) in carrying out its activities. In general, these are the **information** which are created and stored as a result of Absa's business dealings and activities.
Relevant Record	Records which must be sourced, created, retained, and managed in a manner that are compliant with specific legal, regulatory, or business requirements (e.g. operational business purposes, demonstrate policy compliance). Records that are considered relevant are identified in Country Retention Schedule(s) which also prescribes the period for which these records should be retained.
Retention Period	The period a relevant data and record/s is required to be retained for Legal and Regulatory purposes.

Definition	Explanation
Source System	Any system or file that captures or holds data of interest. Data is extracted from a source system to send to target systems for further use. In integration terminology this may also be called a **Data Provider** or **Interface Provider**.
SPV	A special purpose vehicle is a separate legal entity created for a specific limited purpose. For example: SPVs can be used to ring fencing assets or debt, or for securitization transactions
Taxonomy	A classification or categorisation of concepts (or things). It contains formal naming and definition of these but is generally limited to a hierarchy or grouping rather than describing all relationships between them. Taxonomies help us to organise and locate things.
Technical Lineage	A subset of the broader **Business Lineage** and pertains only to the integrations and data movements between the systems but has a higher level of detail (akin to the difference between a conceptual and a logical data model). It is preferred that technical lineage be accomplished through self-documenting code and frameworks (such as spline), and not re-written in a separate artefact.
Unique Data Source	A data source that is unique to a business area/ Function and is not deemed a Golden or an Authoritative Source.

5. RECORD OF VERSION CONTROL / UPDATES

Date	Author / Source	Change
15 July 2020	Email from Tina Singh Circular date: 22 October 2019 Circular number: 900/2019	New: Data and Records Management Policy • Version 1.0
23 July 2020	Email from Tina Singh Circular date: 23 July 2020 Circular number: 718/2020	Annual review • Version 2.0
1 September 2021	Email from Morlene Naicker Circular date: 1 September 2021 Circular number: 1236/2020	Annual review with a name change: • Name changed from Data and Records Management Policy to Data and Records Management Risk Policy • Version 3.0
29 June 2022	Krisantha Naidoo - PCM Custodian	• Links updated to Policy Hub • Review date extended to 30 September 2023