Risk Data Aggregation and Risk Reporting (RDARR) Policy

INTERNAL ONLY

Governance	
In support of the following Principal Risk Framework	Enterprise Risk Management Framework
Principal Risk	Non-Risk Type Specific
Sub Risk Type	Not Applicable
Approval date	10 March 2023
Last review date	10 March 2023
Next review date	10 March 2024
Location	Policy Hub> Policy Documents

Ownership	
Accountable Executive (Group CRO)	Deon Raju Designation: Absa Group Limited Chief Risk Officer
Risk Type Officer	Not Applicable
Sub Risk type Owner	Not Applicable
Policy Owner (RTO or delegated official)	Phiwe Soldati Designation: Risk Chief Operating Officer
Policy Approver	Phiwe Soldati Designation: Risk Chief Operating Officer
Policy Custodian (Contact)	Cindy Stringer Designation: Head: Enterprise Risk Reporting

TABLE OF CONTENT

Risk Data Aggregation and Risk Reporting (RDARR) Policy

1. POLICY CONTEXT

1.1 Introduction

The Risk Data Aggregation and Risk Reporting (RDARR) Policy, hereafter referred to as the 'RDARR Policy', 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. The objective is to help the Board and Executive Management make better informed decisions when using risk data, to understand the quality of risk data and risk reporting, and to take appropriate decisions and actions to improve upon risk data aggregation and risk reporting.

This Policy is in support of the Enterprise Risk Management Framework (ERMF) and operates in tandem with the Data and Records Management Risk Policy. This Policy must 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 RDARR Policy are to:

- Provide an overview of RDARR;
- Define the minimum control objectives for the aggregation and reporting of risk data and overarching governance and IT infrastructure requirements; and
- Provide requirements applicable to RDARR control practices.

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 the 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 Limited 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 are not in scope for this policy as the Supplier Control Obligations (SCO's) control requirements will apply. The only exception is if a consultant is seconded to Absa Group Limited

(c) Legal entities as envisaged in the Entities in Scope for Risk Data Aggregation and Risk Reporting Standard.

1.3.2 Out of Scope

This policy does **not** apply to:

(a) 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

(b) 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."

- Any business units or risk types that are not governed by the Basel Commission on Banking Supervision (BCBS).

- For out of scope entities and functions that provide information into the in-scope risk metrics, an attestation is required to attest to the quality of the data provided on each occasion that data is provided. The data is in-scope from this point onwards.
- Regulatory calculations and reporting as specified or required by regulators other than the South African Reserve Bank (SARB).

  **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 PROVISION / CONTROL REQUIREMENTS

2.1 Overview of the RDARR Policy

This Policy further complements and supplements the requirements defined in the Absa Group Limited Data and Records Management Risk Policy. It also references other policies and standards such as the End User Developed Applications (EUDA) Standard and the Information Security and Cyber Security Policy. This Policy does not aim to duplicate these other policies, but refers to them where necessary to provide context in relation to the BCBS 'Principles for Effective Data Aggregation and Risk Reporting', also known as BCBS 239. These principles are:

- Governance and architecture:
  - Principle 1: Governance
  - Principle 2: Data Architecture and Information Technology Infrastructure
- Risk data aggregation
  - Principle 3: Accuracy and Integrity
  - Principle 4: Completeness
  - Principle 5: Timeliness
  - Principle 6: Adaptability
- Risk reporting
  - Principle 7: Accuracy
  - Principle 8: Comprehensiveness
  - Principle 9: Clarity and Usefulness
  - Principle 10: Frequency
  - Principle 11: Distribution
- Regulators and supervisors:
  - Principle 12: Review
  - Principle 13: Remedial Actions and Supervisory Measures
  - Principle 14: Home/Host Cooperation

2.2 Control objectives and Overarching Governance

This section outlines the minimum control requirements specific to RDARR that complements or expands on the control requirements in the Data and Records Management Risk Policy as applicable for risk data.

2.2.1 Control Statement: Promote risk data quality awareness

2.2.1.1 Control Objective

To ensure that the Board and Executive Management are aware of the data quality risks associated with the information that they receive to make key decisions, Absa Group Limited's overall risk management approach must be extended to include the identification, assessment, and management of data quality risks, as defined in the Risk Data Aggregation and Risk Reporting Limitations Standard.

2.2.1.2 Control Requirement

A process must be established to make the Board and Executive Management aware of any material limitations in the quality of data they receive to make risk-based decisions. The control objectives where relevant to comply with RDARR and references to specific RDARR capabilities detailed in the Data and Records Management Risk Policy and Risk Data Aggregation and Risk Reporting Limitations Standard must be implemented to monitor, manage, and report risk data limitations effectively.

2.2.2 Control Statement: Apply risk data quality standards to service agreements

2.2.2.1 Control Objective

Risk metric Data Owners must ensure that appropriate service (external to the Group or Business Area) or operational (internal) level agreements (SLA or OLA) are in place in order to manage adherence to minimum risk data standards and controls. The requirements of the Data and Records Management Risk Policy should be considered at all points, especially when data enters the risk environment.

An SLA / OLA should be in place between Owners of each data hand off, whether between systems or processes.

To manage the risk associated with risk data service providers external to Absa Group Limited, the provisions of the Group Procurement Policy must also be followed.

2.2.2.2 Control Requirements

Sourcing of risk data from external sources must comply with the Group Procurement Policy to ensure that the risk associated with utilising suppliers to provide services to data processes is understood, monitored and mitigated appropriately, and that data suppliers are managed accordingly to ensure compliance with the ERMF and with relevant legal and regulatory requirements.

Where any of the below information is available in metadata or process documentation tools, the OLAs may make reference to these tools.

Where applicable, all service and operational agreements for risk data related processes should cover the following:

- The owners and stewards for the risk data or processes as appropriate;
- Scope of risk data or process required to produce the risk data or process;
- The dimensions or Critical Data Elements (CDEs) for aggregation through the life cycle of the risk data or process;
- If aggregation occurs the levels of granularity of aggregation are specified;
- Availability of data under normal and stress conditions;
- Timeliness and frequency of data;
- Materiality thresholds for data accuracy (the data from source has been loaded into the target without unintentional content changes), completeness (no records have been lost), timeliness (data is supplied in the required timeframe), availability (data is available to the required users), portfolio coverage (the data contains all the required records for the portfolio) and consistency (data structure and format remains uniform over time) as appropriate;
- Reporting of issues and limitations through relevant governance processes and the provision of the necessary information relating to relevant limitations for escalation as per the Risk Data Aggregation and Risk Reporting Limitations Standard as well as the Data and Records Management Risk Policy; and
- Assigned roles and responsibilities to monitor service levels, escalate (per the thresholds or other agreed point), remediate and resolve material issues.

Note that where items above are not applicable this should be stated as such.

2.2.3 Control Statement: Apply independent validation to RDARR practices

2.2.3.1 Control Objective

To ensure that risk data aggregation capabilities and risk reporting processes are subject to strong governance, independent validation of risk data aggregation and reporting capabilities must be aligned to and integrated with other independent assurance activities.

2.2.3.2 Control Requirement

Independent validation of the RDARR processes and controls must be performed across the three lines of defence, using the relevant components of the Combined Assurance model, according to the approved ERMF and Assurance Standard.

2.2.4 Control Statement: Apply RDARR Practices to new products, initiatives, acquisitions, system and process changes, including regulatory changes

2.2.4.1 Control Objective

All risk data aggregation capabilities and risk reporting practices must be considered as part of any new initiative, including acquisitions and / or divestitures, new product development or product amendment, additional requested risk metrics, as well as broader process and IT change initiatives. The requirements of the Project Change Risk Policy, Product Delivery Lifecycle (PDLC) Standard, Product Risk Standard and the Business Collaboration Policy as they relate to RDARR practices should be considered.

2.2.4.2 Control Requirements

- Any new or amended product or business initiative or acquisition is required to go through a formal approval process before it is implemented in accordance with the policies listed above.
- Business Area product, initiative or acquisition approval processes must include an assessment of the potential impact to risk data aggregation and reporting capabilities prior to going live, including data lineage, authoritative data source (ADS), unique data source or core data platform, and control requirements specified in this Policy.
- Results of the assessment and any identified remedial actions must be approved by the data and process owners. Gaps against compliance with this Policy are required to have remedial actions agreed upon and tracked as part of the approval. Remaining gaps must be reported in line with the Management of Dispensations, Waivers and Breaches Standard.
- Process Owners whose processes and procedures include, contribute to, or form part of risk reporting must ensure that those processes and procedures are kept under change control.
  - Where any change, whether through acquisition, business strategy, product set, or processes is being made to the technology solutions involved in operating those processes and procedures, the relevant Process Owner is accountable and the Process Steward responsible, for ensuring that the changes are adequately defined, tested, deployed and put to use in such a way that RDARR practices control requirements are met at all times.
  - Evidence must be retained for 12 months with respect to assured delivery on expected outcomes (including testing strategies, test plans and test results).
  - Any material changes to processes must be reflected in the process documentation.

2.2.5 Control Statement: Apply RDARR Practices to changes in the ERMF

2.2.5.1 Control Objective

In order to maintain RDARR compliance, all risk data aggregation capabilities, and risk reporting practices should be applied to the key data metrics and reporting of principal risks specified in the ERMF as determined to be in-scope by the Group Risk and Capital Management Committee (GRCMC).

2.2.5.2 Control Requirement

- On an annual basis, the risk metrics and board and executive committees which are determined to be in-scope for RDARR compliance should be confirmed by the GRCMC.
  - Metrics which are newly determined to be in-scope have a 12 month period to meet the requirements of this Policy.
- Principal risks which have been added or amended during the annual ERMF review are required to go through a formal approval process to confirm compliance with this Policy within a 12 month period.
  - An assessment should be performed to determine which key data metrics are reported to the board and executive committees. These metrics should be considered in-scope metrics and the committees, the in-scope committees.
  - The business area then has a 12 month period to meet the requirements of this Policy.

2.2.6 Control Statement: Maintain RDARR practices irrespective of organisational structure

2.2.6.1 Control Objective

The RDARR capabilities should not be hindered by group structure at any level and should be independent from the choices the organisation makes regarding its legal and geographical structure.

2.2.6.2 Control Requirement

Changes to the legal and geographical structure of the group should not prevent effective deployment of risk aggregation and reporting practices.

2.2.7 Control Statement: Embed limitations process with Executive Management and the Board

2.2.7.1 Control Objective

A Limitations Process must be established to enable Executive Management and the Board to make informed decisions based on the risk data they receive as well as to ensure that they are fully aware of, understand, and actively manage those limitations that materially impact and prevent full risk data aggregation and reporting.

2.2.7.2 Control Requirement

The limitations control requirements are specified in the Risk Data Aggregation and Risk Reporting Limitations Standard. The controls which must be implemented include:

- Facilitate the implementation of a consistent limitations process across the end-to-end RDARR value chain.
- Define materiality and criticality thresholds for data to enable the assessment of the impact of the limitations and the aggregation of limitations.
- Determine the severity of the limitations by applying a suitable criticality assessment of the impact of limitations raised according to the principles defined in the Risk and Issue Classification Standard.

2.2.8 Control Statement: Consider risk data aggregation capabilities and risk reporting processes, in business resilience and continuity planning

2.2.8.1 Control Objective

In order to support its risk data aggregation capabilities and risk reporting practices fully, the organisation's business resilience plans must include processes and activities to aggregate risk data and requirements for risk reporting in times of organisational stress, whether idiosyncratic (bank specific) or systemic. Plans must include an agreed approach to interim or ad hoc reporting in times of stress, the processes and activities required to produce key metrics, any resource interdependencies and the CDEs required for risk data aggregation.

Risk data aggregation processes must be subject to regular business impact assessments including, where appropriate, simulated disaster recovery tests. Weaknesses or limitations discovered in these tests must be addressed and incorporated into relevant Business Continuity and Resilience Plans.

2.2.8.2 Control Requirement

Business Areas must ensure their business recovery and resilience plans incorporates all applicable RDARR capabilities and criteria as defined in the Risk Reporting Standard.

2.2.9 Control Statement: Develop integrated risk data taxonomies

2.2.9.1 Control Objective

The Data Owners are accountable for ensuring that an integrated risk data taxonomy and data glossary are established to ensure that a uniform classification of risk data is applied across the organisation.

2.2.9.2 Control Requirements

- Data Owners are accountable and Data Stewards responsible for ensuring that the risk metric and data definitions are incorporated in the Business Glossary, with reference to the Data and Records Management Risk Policy, as per Control Statement: Develop integrated risk data taxonomies and maintained.
- The Data Owners are accountable for:

- Defining and publishing the definitions in a central data glossary in line with the requirements detailed in the Data and Records Management Risk Policy, and
- Ensuring that the business glossary is available and accessible.

Each business area must consistently implement the taxonomy across functions and domains in line with the objective of establishing reliable and accurate data that is available, accessible, consistent, and accurate, which aligns to the criteria set out in the Data and Records Management Risk Policy.

2.2.10 Control Statement: Document the RDARR lineage

2.2.10.1 Control Objective

Data lineage provides traceability of the data chain to help identify unique and authoritative data sources and data transformations. Appropriate controls must be applied to relevant risk metrics and CDEs to ensure that data ownership is identified throughout the data lifecycle, from source to final reporting, and the data quality thresholds are met in the context of RDARR.

The nature and characteristics of systems, data, models, controls and responsibilities of the RDARR process must be documented, owned and maintained.

2.2.10.2 Control Requirement

Risk Data and Process Owners are accountable for, and Stewards responsible for, ensuring that the end-to-end data lineage (from where the data is received, and processed until it is provided to a consumer), is fully documented in line with the Data and Records Management Risk Policy.

2.2.11 Control Statement: Establish an end-to-end risk data ownership model

2.2.11.1 Control Objective

To ensure effective data management, oversight and remediation, an end-to-end risk data ownership model must be established with clearly defined roles and responsibilities as they relate to the ownership and quality of risk data and information, throughout the risk data lifecycle.

The importance of articulating the roles and responsibilities and establishing business and IT owners, is to ensure a thorough understanding of the nature and characteristics of the data, the quality of the data, the data's lineage and the data risks and associated controls by Data Owners and Data Stewards.

2.2.11.2 Control Requirements

- Data Owners must ensure the integrity of risk data captured into the risk processes (point of origination), as well as assuring that the organisation's risk aggregation and reporting capabilities remain consistent with approved risk policies.
- The Head of the Business or Risk Area must appoint a Data Owner for CDEs within the organisation as defined in the Data and Record Management Policy. Data Owners may appoint Data Stewards.
- Data Owners are accountable and Data Stewards responsible for the accurate transformation and calculation of each in-scope risk metric as used for decision-making or risk appetite monitoring.

2.3 Risk Data Aggregation and Reporting Control Practices

2.3.1 Control Statement: Implement an approved data source for the sourcing of and reporting on each risk type or risk area

2.3.1.1 Control Objective

To facilitate the aggregation and calculation of, and access to, accurate and reliable risk data, an ADS, unique data source or a core data platform must be identified and implemented for the sourcing of risk data or reporting of each risk type or risk area, as appropriate, in accordance with the Data and Records Management Risk Policy.

2.3.1.2 Control Requirements

An ADS, unique data source or core data platform is a recognised and trusted data source to publish reliable and accurate data for subsequent use by other systems and users.

- The Data Owners and Stewards are accountable and responsible for ensuring that the CDEs utilised in the production of the risk metric are sourced from an ADS, unique data source or a core data platform per risk type in accordance with the Data and Records Management Risk Policy.
- The Data Owners and Stewards are accountable and responsible for ensuring that the risk metrics are stored in an ADS, unique data source or a core data platform for the relevant risk type.
- The ADS, unique data sources and core data platform must have sufficient controls to ensure that the data within these sources meets data quality requirements, as detailed in the Data and Records Management Risk Policy.
- While an ideal state would be to have a single ADS for a data domain with enterprise-wide scope, this is not always possible or advisable. Therefore, at the Architecture Council's discretion, a unique data source or core data platform may be used. All requirements in order to meet the definition of a unique data source or core data platform must be met in line with the Data and Records Management Risk Policy.

2.3.2 Control Statement: Apply EUDA controls to manual processes and desktop applications

2.3.2.1 Control Objective

To ensure accurate calculations and limited output errors, all End User Developed Applications (EUDA) and manual processes created and used for risk data aggregation and reporting must be identified, collated in an inventory and assessed for criticality as required by the End User Developed Applications (EUDA) Standard.

2.3.2.2 Control Requirements

- Process Owners and Stewards must identify EUDAs, collate them in an inventory, assess them for criticality, and comply with the applicable critical control requirements as specified in the End User Developed Applications (EUDA) Standard.
- EUDA criticality assessments must demonstrably consider the risk of inaccurate risk data aggregation and include appropriate actions to reduce the impact.

2.3.3 Control Statement: Reconcile risk data to finance data and to the ADS unique data sources or core data platform

2.3.3.1 Control Objective

To ensure the accuracy of risk data, it must be reconciled to the equivalent financial data, where appropriate. In addition, risk data must also be validated for accuracy and unauthorised or inappropriate changes against the approved ADS, unique data sources or core data platform as required by the Risk and Finance Data Alignment and Reconciliation Standard.

2.3.3.2 Control Requirements

- Process Owners who are accountable and Stewards who are responsible for the aggregation of risk data, must execute a process to ensure that the data is accurately reconciled to equivalent financial data if appropriate, and / or to an authorised source, in line with the reporting frequency.
- Results of the data reconciliations must be monitored, items compared and differences in outcomes must be reported, explained and remediated in a timely manner.

- Any Risk and Finance Data Alignment (RAFDA) applied to the data must be captured in a RAFDA Register and, if manual, also within an adjustments register to explain the differences in the data.
- The Data Owner is accountable, and the Data Steward responsible, for reviewing any manual adjustments made to the risk metric, to determine if the adjustments are appropriate.
- Limitations arising from RAFDAs must be reported in line with the Risk Data Aggregation and Risk Reporting Limitations Standard.

2.3.4 Control Statement: Check that risk data is complete, available, accurate and timely

2.3.4.1 Control Objective

- The Board and Executive Management must have confidence that their risk decisions are based on data that is complete, accurate and timely. Exceptions must be managed in such a way that they do not significantly impact the organisation's ability to manage material risks.
- All material risks must be identified, including off-balance sheet exposures and approximations. These must be included in the RDARR processes.
- In order to meet risk management reporting requirements, risk data aggregation capabilities must be sufficient to produce timely aggregate risk information, both in business as usual and in response to a stress event as defined in the applicable SLA or OLA.

2.3.4.2 Control Requirements

- Data Owners must communicate data quality issues relating to completeness, availability, accuracy, consistency, validity and timeliness through the appropriate processes, in accordance with the Data and Record Management Policy.
- The Data Owner is required to communicate any material limitations in the completeness, availability, accuracy and timeliness of risk data, as per the Risk Data Aggregation and Risk Reporting Limitations Standard.
- The Head of the Business Area or Risk Area is accountable for implementing the Absa Group Limited approach for limitations reporting as per the Risk Data Aggregation and Risk Reporting Limitations Standard.
- The Head of the Business Area or Risk Area is accountable for the communication and monitoring of resolution of limitations relevant to the risk type, to the Enterprise Limitations Process, as per the Risk Data Aggregation and Risk Reporting Limitations Standard.

2.3.5 Control Statement: Risk data aggregation capabilities must be flexible, scalable and adaptable

2.3.5.1 Control Objective

The risk data infrastructure and architecture must be designed and implemented in a manner that is adaptable, scalable and extensible to support ongoing business needs, new initiatives and emerging risks, including the ability to aggregate and report on data accurately and consistently in an automated manner wherever practical.

2.3.5.2 Control Requirements

The Data Owner must ensure that the risk and business area processes and technology requirements include the ability to perform out of cycle reporting (including fire drills and adhoc reporting), data analyses, data customisation, and inclusion of new initiatives in a timely manner, as per the Control Statement: Apply RDARR practices to new initiatives, and that these requirements are considered throughout the lifecycle of the IT Strategy.

- The Data Owner and Data Stewards must ensure that RDARR requirements are included in any change initiative.
- The Data Owners for risk metrics need to specify the dimensions that each metric is required to be aggregated and reported on for both business as usual and for out of cycle (including fire drills and adhoc reporting), to ensure that data is available at the required level of granularity.
- The Data Owners are accountable and Stewards responsible for ensuring that the requirements are made available in the ADS, unique data source or core data platform to allow for aggregation and reporting at the required level of granularity.
- The Process Owners and Process Stewards must conduct an annual review of the RDARR process documentation, to ensure that it is still applicable and reflects the current processes.

- Report Owners and Report Stewards are to adhere to the use of defined reporting processes, actioning of controls and using the approved architecture when reporting within a business as usual or as part of out of cycle reporting requests (including fire drills and adhoc reporting. Where this is not possible the Process Owners and Stewards must be made aware. Refer to the Risk Reporting Standard for risk reporting requirements.
- The Report Owners and Report Stewards must conduct an annual qualitative assessment (internal fire drill exercise) on adaptability of risk data to respond to:
  - Ad hoc requests for risk reporting received during the prior period;
  - Reporting in times of stress;
  - Requests to make amendments to normal reporting in a timely manner; and
  - Adaptability for evolving requirements.

2.3.6 Control Statement: Apply data quality controls to risk reporting

2.3.6.1 Control Objective

To ensure that the Board and Executive Management can confidently rely on the aggregated information to make critical decisions about risk, risk management reports must adhere to data quality controls relating to accuracy, precision, completeness and timeliness.

2.3.6.2 Control Requirements

The risk reporting processes must be documented as per Control Statement: Document the RDARR lineage.

The Data Owners are accountable and the Data Stewards responsible for ensuring that relevant controls are implemented on the risk data aggregation processes to identify, communicate, and remediate issues relating to accuracy, precision, completeness, and timeliness, as per the following RDARR Policy control statements:

- Control Statement: Reconcile risk data to finance data and to the Authorised Source.
- Control Statement: Ensure risk data is complete, accurate and timely.

The Report Owners and Stewards and Process Owners and Stewards are accountable and responsible for ensuring that the above controls are also implemented on the risk reporting processes and that the limitations are reported appropriately.

2.3.7 Control Statement: Ensure risk management reports are comprehensive, clear, relevant, useful and distributed to the correct recipients at the required frequency

2.3.7.1 Control Objective

Risk management reports must cover all material risk areas within the organisation, be clear, relevant, and received in time to allow for timely and effective decision making. The depth and scope of reports must be consistent with the size and complexity of the organisation's operations and risk profile, as well as the requirements of the recipients. Risk management reports must include an appropriate balance of quantitative risk data and qualitative commentary, as determined by the relevant committee. The reports must be published to an approved list of recipients.

2.3.7.2 Control Requirements

The Risk Management, Executive and Board Committees are responsible for defining the scope, quality, frequency and distribution requirements of their risk reports.

The Report Owners are accountable, and the Report Stewards responsible for:

- Maintaining a register of report users, and reviewing this list at least annually;
- Ensuring that the scope, quality, frequency and distribution requirements of the risk reports are reviewed with users at least annually; and
- Ensuring that the clarity and usefulness of the reports are assessed at least annually with the report users.

3. POLICY GOVERNANCE

3.1 Roles and responsibilities

Roles and responsibilities are articulated in this policy, as they relate to the ownership and quality of risk metrics, risk data, risk reports and controls to be implemented throughout the RDARR value chain.

Key roles and responsibilities to achieve the Policy requirements:

ROLE	RESPONSIBILITY
In-scope Board, Executive and Risk Management Committees	• Oversee Executive Management's ownership and implementation of RDARR principles. • Define the risk reporting requirements most suitable for the size, nature and complexity of the bank's operations. • Approve risk appetite metrics and dimensions required to be reported on to the relevant committee. • Define the scope, quality, frequency and distribution requirements of their risk reports. • Assess their risk reporting requirements at least on an annual basis and provides feedback to the report owners regarding the comprehensiveness, relevance, scope, clarity, frequency, distribution and quality of the risk reports. • Acknowledge awareness of limitations of risk data aggregation upon consumption of the Board Risk reports, as per the Risk Data Aggregation and Risk Reporting Limitations Standard. • Promote the identification, assessment and management of data quality as part of the ERMF. • Approve the recommended in-scope RDARR set of metrics, committees, entities and reports.
Absa Group Limited Chief Risk Officer (CRO)	• Accountable for the Enterprise wide management of risk data aggregation capabilities and risk reporting processes. • Rationalise, plan for and implement the automation of relevant manual activities, in conjunction with the Data Owners, for Enterprise aggregated risk metrics. • Determine and communicate the materiality level of risk portfolios reported on at Exco and Board level using Risk and Issue Classification Standard guidance. • Conclude on what is or is not included in the scope for RDARR (including metrics, committees and reports) for recommendation to the in-scope Board committee.
Risk Type Officer (RTO)	• Accountable for RDARR, for the risk type. • Responsible for implementing the RDARR Policy within the Risk Type. • Determine the key risk type metrics for inclusion in RDARR processes. • Act as or appoint a Data Owner for own principal risk type key metrics. • Rationalise, plan for and implement the automation of relevant manual activities, in conjunction with the Data Owners, for risk-type risk metrics. • Accountable for implementing the Absa Group Limited approach for limitations reporting as per the Risk Data Aggregation and Risk Reporting Limitations Standard. • Accountable for the communication and resolution of limitations relevant to the risk type, to the Enterprise Risk Reporting team, as per the Risk Data Aggregation and Risk Reporting Limitations Standard. • Accountable for implementing the Reporting Standard as appropriate.
Business Area Chief Risk Officer (BA-CRO)	• Accountable for RDARR for the business area. • Responsible for implementing the RDARR Policy within the Business Area. • Act as or appoint a Data Owner for each identified CDE that is used in the production of a risk appetite metric.

ROLE	RESPONSIBILITY
	• Make sure that limitations are remediated in accordance with organisation change appetite.
Data Owner	• Appoint Data Stewards where applicable as delegates who will have day-to-day operational responsibility over the risk data. • Confirm that appropriate service (external) or operational (internal) level agreements are in place in order to manage adherence to minimum risk data quality standards and controls. • Accountable for ensuring that the risk metric and data definitions are incorporated in the Business Glossary. • Accountable for publishing the definitions in a data glossary in line with the control requirements detailed in the Data and Records Management Risk Policy. • Accountable for ensuring that the business glossary is available and accessible. • Communicate data quality issues relating to completeness, accuracy and timeliness through the respective business data issues / limitations reporting structure as well as consumers of the data, in accordance with the Data and Records Management Risk Policy and associated Standards. • Accountable for ensuring requirements are made available in the ADSs, unique data sources or a core data platform to allow for aggregation and reporting at the right level of granularity. • Accountable for ensuring that relevant controls are implemented on the risk data aggregation processes to identify, communicate and remediate issues relating to accuracy, availability, precision, completeness and timelines. • Accountable for reviewing any manual adjustments made to the risk metric, to determine if the adjustments are appropriate. • Communicate any material limitations in the completeness, accuracy and timeliness of risk data, as per the Risk Data Aggregation and Risk Reporting Limitations Standard. • Confirm that the risk reporting processes and technology requirements include the ability to perform ad hoc reporting, data profiling in a timely manner, data customisation, and inclusion of new initiatives. • Confirm that change initiatives when in scope for RDARR, meet RDARR control objective. In addition, the following apply for Data Owners of risk metrics: • Specify the dimensions that each metric is required to be aggregated and reported on, to ensure that data is available at the right level of granularity. • Accountable for accurate transformation and calculation of each risk metric. • Accountable for ensuring that risk data utilised in the production of the risk metric is stored in and sourced from an ADS, unique data source or a core data platform, per the Data and Records Management Risk Policy. • Define clear operational data ownership and accountability for critical risk data with Data Owner(s) appointed for each business domain.
Data Steward	• Responsible for ensuring that the risk metric and data definitions are incorporated in the Business Glossary. • Responsible for ensuring requirements are made available in the ADS, unique data source or core data platform to allow for aggregation and reporting at the right level of granularity. • Responsible for applying controls for ensuring that the risk data in the ADS, unique data source or core data platform is reconcilable back to the source systems, with a process in place to identify, track and remediate differences.

ROLE	RESPONSIBILITY
	• Responsible for reviewing any manual adjustments made to the risk metric, to determine if the adjustments are appropriate. In addition: the following apply for Data Stewards for risk metrics: • Responsible for the accurate transformation and calculation of each key risk metric as used for decision-making or risk appetite monitoring. • Responsible for ensuring that risk data utilised in the production of the risk metric are sourced from an ADS, unique data source or core data platform, according to the requirements of the Data and Records Management Risk Policy.
Report Owner	• Accountable for maintaining a register of report users and reviewing this list annually or in the event of changes to the composition of the relevant committee. • Accountable for ensuring that the scope, quality, frequency and distribution requirements of the risk reports are reviewed with users at least annually. • Conduct an annual qualitative assessment (internal fire drill exercise) on adaptability of risk data to respond to: – Ad hoc requests for risk reporting received during the prior period; and – Requests to make amendments to normal reporting in a timely manner. • Accountable for ensuring that the above controls are also implemented on the risk reporting processes. • Accountable for ensuring that reporting is based on defined processes, controls and approved architecture in reporting scenarios (business as usual, ad hoc reporting and times of stress).
Report Steward	• Responsible for maintaining a register of report users and reviewing this list annually or in the event of changes to the composition of the relevant committee. • Responsible for ensuring that the scope, quality, frequency and distribution requirements of the risk reports are reviewed with users at least annually. • Conduct an annual qualitative assessment (internal fire drill exercise) on the adaptability of risk data to respond to: – Ad hoc requests for risk reporting received during the prior period; and – Requests to make amendments to normal reporting in a timely manner. • Responsible for ensuring that the above controls are also implemented on the risk reporting processes. • Responsible for reporting based on defined processes, controls and approved architecture in reporting scenarios (business as usual, ad hoc reporting and times of stress).
Process Owner	• Appoint Process Stewards. • Accountable for any change, i.e business strategy, acquisitions, product set or processes and procedures. • Accountable for ensuring developed or acquired solutions are adequately defined, tested, deployed and put to use in such a way that Risk Data Aggregation control requirements and Risk Reporting Practices control requirements are met at all times. • Accountable for ensuring the end-to-end risk data lineage, from where the data is received, and processed until it is provided to a consumer, is fully documented in line with the requirements of the Data and Records Management Risk Policy. • Identify EUDAs, collate them in an inventory, assess them for criticality, and comply with the applicable criticality control requirements as specified in the End User Developed Applications (EUDA) Standard.

ROLE	RESPONSIBILITY
	• Accountable for the execution of a process to ensure that the data is accurately reconciled to equivalent financial data if appropriate, and / or to an ADS, unique data source or a core data platform, in line with the reporting frequency. • Accountable for conducting an annual review of the RDARR process documentation, to ensure that it is still applicable and reflects the current processes. • Accountable for ensuring that controls are also implemented on the risk reporting processes.
Process Steward	• Responsible for ensuring that any change is managed in line with prevailing Critical Process Assessment (CPA) requirements and technology standards. • Responsible for ensuring developed or acquired solutions are adequately defined, tested, deployed, and put to use in such a way that Risk Data Aggregation control requirements and Risk Reporting Practices control requirements are met at all times. • Responsible for ensuring the end-to-end risk data lineage, from where the data is received, and processed until it is provided to a consumer, is fully documented in line with the requirements of the Data and Records Management Risk Policy. • Identify EUDAs, collate them in an inventory, assess them for criticality, and comply with the applicable criticality control requirements as specified in the End User Developed Applications (EUDA) Standard. • Responsible for the execution of a process to ensure that the data is accurately reconciled to equivalent financial data if appropriate, and / or to an ADS, unique data source or a core data platform, in line with the reporting frequency. • Responsible for conducting an annual review of the RDARR process documentation, to ensure that it is still applicable and reflects the current processes. • Responsible for ensuring that controls are also implemented on the risk reporting processes. • Accountable and responsible for assessing the trade-offs to meet one of the control objectives over another.

3.2 Adherence

- The provisions / control requirements of this policy are mandatory and are used to implement a group-wide approach for managing RDARR 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.
- Where, due to exceptional circumstances a trade-off or compromise is required to meet one of the control objectives over another, especially during ad hoc reporting or reporting in times of stress, the impact of the trade-off on risk-decision making should be assessed prior to being applied. If the trade-off is material, it should be reported to Executive Management and to the GRCMC. The Process Owner is accountable and responsible for assessing the trade-offs. A record of all trade-offs should be maintained.
- Business areas, Risk, and Finance heads must conduct an annual self-assessment review to assess completeness and sufficiency of RDARR risk management in their areas and identify whether RDARR risk coverage, under their Combined Assurance Model in line with the ERMF, is adequate or must be further expanded to enhance and streamline the risk measurement and management processes. The result of such annual review must be communicated in writing to the Absa Group Limited Chief Risk Officer.
- 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 policy, the frameworks, policies and standards of other Principal Risks – as detailed within the ERMF – may apply and interact invariably to the requirements set out in this policy and are to be complied with.

3.4 Reputational Impact

Any action or inaction taken relevant to this policy which may have 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 Committee in accordance with the Reputation Risk Policy.

3.5 Data Privacy

For all personal data that is collected, processed, stored, shared, archived or destroyed under this Policy, 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 Policy 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 to colleagues 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 in accordance with this Code of Ethics and the policies that apply to their roles. Any failure to act in accordance with the Values and Behaviours or breaches 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 and select Policies and Standards:
  - Risk and Issue Classification Standard
  - Assurance Standard
  - Process Risk Management Policy
- Information Security and Cyber Risk Policy
- Data and Records Management Risk Policy
- End User Developed Applications (EUDA) Standard
- Group Procurement Policy
- Entities in Scope for Risk Data Aggregation and Risk Reporting Standard
- Risk Reporting Standard
- Risk Data Aggregation and Risk Reporting Limitations Standard
- Risk and Finance Data Alignment and Reconciliation Standard
- Group Risk Appetite Framework
- Project Change Risk Policy
- Product Delivery Lifecycle (PDLC) Standard
- Product Risk Standard
- Business Collaboration Policy
- Business Continuity Management (BCM) Risk Policy
- Management of Dispensations, Waivers and Breaches Standard
- Data Privacy Policy

- Data Privacy 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
ADS	Authoritative Data Source
BA	Business Area
BCBS	Basel Committee on Banking Supervision
CDE	Critical Data Element
CRO	Chief Risk Officer
ERMF	Enterprise Risk Management Framework
EUDA	End User Developed Application
GRCMC	Group Risk and Capital Management Committee
IFRS	International Financial Reporting Standards
IT	Information Technology
OLA	Operational Level Agreement
RTO	Risk Type Officer
RAFDA	Risk and Finance Data Alignment
RDARR	Risk Data Aggregation and Risk Reporting
SLA	Service Level Agreement

4.2.2 Definitions

Definition	Explanation
Authoritative Data Source	A recognized and trusted data source, from which to publish reliable and accurate data for subsequent use by other systems and users.
Business Area	Everyday Banking (EB), Product Solutions (PS), Relationship Banking (RB), Corporate and Investment Bank (CIB), Absa Regional Offices (ARO), Countries and Sub-Business Area
Country and Legal Entity	Countries and Legal Entities falling within the Group structure
Critical data element	Critical Data Elements are any data elements that are 'critical to success' for the business. In the case of elements that are derived / calculated from other elements, both the calculated element and the underlying elements used for the calculation must be considered as Critical Data Elements (e.g. Probability of Default, Risk-Weighted Assets etc.) In the context of the interpretation by this Policy, both risk metrics and risk indicators are deemed critical data.
Data	Within Absa Group Limited, Data is defined in terms of a Critical Data Element (the most granular unit of data (e.g. Trade Price, Trade Amount etc.) for which the definition, identification, representation, and permissible values are specified) and Data Domains (a collection of Critical Data Elements e.g. Trade).

Definition	Explanation
Dimension	An attribute by which a metric is grouped, e.g. legal entity, country code, industry code, etc.
Group Functions	Engineering Services, Risk, Finance, Tax, Compliance, Legal, Marketing and Corporate Relations, Treasury, Human Resources and Internal Audit
Limitation	A constraint that prevent accurate RDARR of Absa Group Limited's risk profile relative to its approved risk appetite. Limitation types are detailed in the introduction to this document
Risk appetite	The maximum level of risk and the types of risk that the institution is willing to tolerate. This is articulated using quantitative and qualitative risk appetite statements.
Risk data	For the purpose of this Policy, the term "Risk Data" refers to Data Domains and their associated CDEs used in the calculation and reporting of key risk metrics. This includes the individual data elements (inputs) that are used in the production / calculation of a key risk metric as well as the key risk metric themselves.
Risk data aggregation	Defining, gathering and processing risk data according to Absa Group Limited's risk reporting requirements to enable Absa Group Limited to measure its performance against its risk appetite. This includes sorting, merging, or breaking down sets of data.
Risk metric	Defined in terms of the attribute of risk that is being measured. Attributes of risk include exposure and volatility. Risk appetite is set based on desired and maximum acceptable levels of a risk expressed in the form of a risk metric. Performance relative of risk appetite is measured in terms of risk metrics. Risk metrics typically take one of three forms: • those that quantify exposure; • those that quantify uncertainty; • those that quantify exposure and uncertainty in some combined manner. *Within Absa Group Limited risk metrics (e.g. Economic Capital, Regulatory Capital, Earnings at Risk) used to measure performance relative to risk appetite, quantify exposure and appetite in a combined manner.*
Risk report	A collection of risk data designed to be used for management / board risk decision making or regulatory reporting.
Service level standard	Service level standards are defined standards that must be specifically adhered to and managed with internal and external service providers supplying risk data. They are the minimum service level standards that need to be encompassed in each service level agreement in place with each risk data supplier.
Unique Data Source	A unique data source as defined within the Data and Records Management Risk Policy is a data source that is unique to a business area / function and is not deemed a Golden or an Authoritative Source and is subject to control requirements as outlined in the policy

5. RECORD OF VERSION CONTROL / UPDATES

Date	Author / Source	Change
7 December 2016	Email: Caryn Davies Circular date: 7 December 2016 Circular number: 921/2016	New: Risk Data Aggregation and Risk Reporting (RDARR) Policy • Version 1.0
14 December 2017	Email: Johan de Wet Circular date: 14 December 2017 Circular number: 951/2017	Annual review with updates: • Alignment to Plc DARCs and BAGL Data Management Policy and associated standards. • Clarification and expanded Roles and Responsibilities in response to SARB Guidance Note 2/2017. • Reference to an associated Risk Data Aggregation and Risk Reporting Limitations Standard. • Reference to existing associated BAGL policies and standards. • Version 2.0
28 October 2019	Email: Cindy Stringer Circular date: 28 October 2019 Circular number: 927/2019	Annual review • Version 3.0
11 December 2020	Email: Cindy Stringer Circular date: December 2020 Circular number: 1435/2020	Annual review • Version 4.0
10 February 2022	Email: Cindy Stringer Circular date: 31 January 2022	Annual review • Version 5.0
10 March 2023	Email: Cindy Stringer Circular date: 10 March 2023 Circular number: TBC	Annual review • Version 6.0