# Risk Reporting Standard

## INTERNAL ONLY

| Governance | |
|---|---|
| **Principal Risk** | Non-Risk Type Specific |
| **Sub Risk Type** | Not applicable |
| **In support of the following Policy/ies** | Risk Data Aggregation and Risk Reporting (RDARR) Policy |
| **Approval date** | 6 May 2022 |
| **Last Review date** | 6 May 2022 |
| **Next Review date** | 6 May 2023 |
| **Location** | Policy Hub>Standards |

| Ownership | |
|---|---|
| **Accountable Executive (Group CRO/Business Unit/Area CRO)** | Deon Raju<br>Designation: Absa Group Limited Chief Risk Officer |
| **Principal Risk Officer** | Not Applicable (Non Risk Type Specific) |
| **Sub Risk type Owner** | Not applicable |
| **Policy Owner** | Phiwe Soldati<br>Designation: Risk Chief Operating Officer |
| **Standard Owner** | Phiwe Soldati<br>Designation: Risk Chief Operating Officer |
| **Standard Approver**<br>**Note *Group Standards – PRO or delegated Official / Business Unit/Area Standards – CRO or Delegated official** | Phiwe Soldati<br>Designation: Risk Chief Operating Officer |
| **Standard Custodian (Contact)** | Cindy Stringer<br>Designation: Enterprise Risk Reporting |

# TABLE OF CONTENTS

# Risk Reporting Standard

## 1. STANDARD CONTEXT

### 1.1 Introduction

The Risk Reporting Standard, hereafter referred to as 'the Standard', specifies the required minimum provisions and controls as per the requirements indicated under Purpose, to ensure that risk reporting is implemented effectively and efficiently. It further specifies the minimum control requirements to ensure transparency and accountability for risk reporting. The objective is to help the Board and Senior Management make better informed decisions when using risk data, to understand the quality of risk data and risk reporting, and to take appropriate decisions to improve upon this.

This standard is in support of the Risk Data Aggregation and Risk Reporting (RDARR) Policy and the Enterprise Risk Management Framework (ERMF) and should be read in conjunction with any document listed in Section 4.1 'Related documentation supporting this Standard'.

### 1.2 Purpose

The primary objectives of the Standard are to:

- Define the minimum standards and control objectives for risk reports;
- Provide the requirements applicable to content and formatting;
- Define the process requirements applicable to Risk reporting
- Highlight the requirements applicable to risk reporting controls.

### 1.3 Scope

#### 1.3.1 In scope

**This Standard applies to:**

- Legal entities as envisaged in the Entities in Scope for Risk Data Aggregation and Risk Reporting Standard;
- Employees and workers of the in-scope entities. 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 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 standard as the Beam control requirements will apply. The only exception is if a consultant is seconded to Absa).

#### 1.3.2 Out of Scope

This standard 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."

(c) Any business area of risk types that are not governed by the Basel Commission on Banking Supervision (BCBS).

(d) 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. STANDARD PROVISIONS / CONTROL REQUIREMENTS

This section outlines the minimum control requirements specific to Risk Reporting that complements or expands on the control requirements in the RDARR Policy.

## 2.1 Risk Reporting Requirements

Business as usual risk reports, as defined within the scope of this document, are produced as per a predefined schedule.

Out of Cycle (OOC) reporting takes place in response to a stress or crisis event, or in response to an ad hoc request. OOC reporting is predominantly on Actual results rather than Forecasts, with an expectation that reporting is delivered on a reduced timeline. OOC risk reporting refers to reporting in the following circumstances:

- Reporting in times of stress/crisis:
  - **Systemic Stress:** Market wide event that impacts the Group.
  - **Idiosyncratic Stress:** Group specific event that impacts the Group.
  - **Resilience Stress:** An event that impacts the Group as envisaged by the Business Continuity Management (BCM) Risk Policy.
- Ad hoc/stress reporting outside of BAU reporting, at the request of internal (e.g. Executive Committee (EXCO) or Board) or external (e.g. South African Reserve Bank (SARB)) stakeholders.

These events may require reporting of new metrics or existing metrics on a more frequent basis. The stress testing process which forms part of the annual integrated plan is not considered to be part of OOC reporting.

## 2.2 Content and Formatting Standards

### 2.2.1 Apply minimum content standards to risk reports

Risk reports contain both quantitative and qualitative risk information. Relevant risk information allows report consumers to make risk decisions to respond to risk positions relative to risk appetite. Risk reports at a minimum, address principal risks.

Risk reports may also include other types of information, such as information on main/material and emerging risks, which may be more or less well-defined, as well as information on projects designed to address the impact of risks that have materialised.

- Reports should be validated and reconciled to ensure that they accurately reflect underlying risk data and the underlying risks.
- Risk reports must cover all principal risk types as well as material emerging risks which may impact the organisation in terms of risk type, industry sectors and risk measures.
- Risk information must be conveyed in a clear and concise manner, and be easily understood by the decision-maker.
- Risk reports must be produced and distributed within an appropriate period to ensure timeliness of information.
- Report audiences must set the frequency of risk reports production and distribution according to their needs and the nature of the risk being covered.
- 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.
- Report consumers need risk data for multiple relevant periods including both historic and forecast.
- Risk management reports must include an appropriate balance of quantitative risk data and qualitative commentary, as determined by the relevant committee.
- Reports must be distributed in a controlled manner so that the right recipients receive the correct reports.

## 2.3 Process requirements

Well managed BAU and OOC reporting processes are the foundation of high quality data and the means by which the quality standards set by consumers of risk reports can be met.

Alignment between the BAU and OOC reporting processes (as far as practicable), through the BA crisis playbooks, should be maintained regularly and tested through the annual OOC process.

#### 2.3.1.1 Business as Usual process

Key requirements that need to be defined for BAU reporting include:

- **The process:** from authoritative data sources through transformation and aggregation to production and delivery of the report, as per the report schedule.
- **The what:** current or additional metrics / critical data elements (CDEs), and dimensions for impacted risk types (credit, market and liquidity risk)
- **The when:** frequency and timing of reporting, including the timing of required inputs from the Metric Owners
- **The how:** business lineage, processes and systems included in the production of metrics
- **The who:** report steward responsible for production and delivery of this report on an going basis
- **The audience:** recipients of the report
- **Limitations**: limitations reports, as per the Data and Records Management Risk Policy and the Risk Data Aggregation and Risk Reporting Limitations Standard, accompany the risk report.

#### 2.3.1.2 OOC reporting process

When a request for an OOC risk report is received by either internal or external stakeholders, the Group Chief Risk Officer (GCRO) will nominate a Risk Reporting Coordinator (RRC) who will be responsible for driving the delivery of the required report. This RRC may be the BAU report owner depending on the request.

If the complexity of either the event giving rise to the request, or the required report is high, the GCRO and RRC may constitute a Risk Reporting Working Group (RRWG) to address the delivery of the report. The RRWG must include representation from all relevant principal risk types and Business Areas (BAs). It is the RRC's responsibility to clearly define terms of reference for the RRWG.

Key requirements that need to be defined for OOC reporting include:

- **The process:** from trigger to production of reporting requirements
- **The what:** current or additional metrics / CDEs, and dimensions for impacted risk types (credit, market and liquidity risk) produced within a "best efforts" time frame
- **The when:** frequency and timing of required OOC report based on an event date
- **The how:** business lineage, processes and systems, together with compensating controls
- **The who:** Risk Reporting Coordinator and Report Owner of the OOC report
- **Acceptable trade-offs**: depending on the nature / urgency of the request, it should generally be possible to make trade-offs between timeliness and accuracy of ad hoc and stress reporting. Trade-offs made should be described in the limitations report accompanying the report.

Trade-offs and limitations that arise in producing the information required in response to an OOC request should be documented, and accompany the information sent to the RRC.

On the completion of an OOC risk report, a self-assessment needs to be performed. The self-assessment criteria in determining whether an OOC BAU firedrill was conducted successfully include, but are not limited to:

- Was the data provided within the requested time?
- Was the firedrill performed in accordance with the BA crisis playbook (process and timelines)?
- If not:
  - Identify components that were not aligned
  - Determine the impact on the accuracy and completeness of the information/data provided
  - Devise an action plan around remediation
- Were processes used as part of the firedrill documented, and re-performance results of the firedrill can be re-performed by an independent person?

### 2.3.3 Document the process

Documentation of the risk report production processes clarifies the inputs and outputs as well as the roles and responsibilities of participants, making it easier understandable for accountable executives.

Every report must have a clear, understandable, approval process to be followed, prior to distribution.

All risk reports must have a clearly defined distribution processes as well as distribution lists, with controls to ensure security and confidentiality.

The risk reporting processes for BAU and ad hoc reporting must be documented. Any process weaknesses identified must be documented and a remediation plan implemented. If this process weakness affects the reporting, this must be raised as a limitation.

The Report Owners and Report Stewards must conduct an annual review of the risk data aggregation and risk reporting process documentation, to ensure that it is still applicable and reflects the current processes.

### 2.3.4 Maintain records

Risk reports must be maintained in accordance with the Data and Records Management Risk Policy .

### 2.3.5 Apply information security classification

Risk reports must be published to an approved list of recipients, and must be classified as secret, confidential or internal, as required by the Information Security and Cyber) Risk Policy.

### 2.3.6 Distribution

An inventory of recipients must be reviewed and updated annually, and aligned to the committees' Terms of References.

The risk report must be disseminated to the in-scope committee's members and attendees in accordance with the distribution frequency set and via appropriate distribution channels (i.e secure and approved).

## 2.4 Risk Reporting Controls

The business needs to ensure that the control requirements, which operate along the three lines of defence, are met to enable data to be available at the required level of performance and reports to be produced both for BAU and in response to OOC reporting.

Accountable executives need to understand the processes used to produce the risk reports for which they are responsible, make reasonable enquiry as to the quality of the information they contain and address any shortcomings or ensure that they are addressed appropriately. Report Owners are accountable and Stewards are responsible for capturing reporting processes and data quality controls in a control inventory.

### 2.4.1 Implement production controls

Given the volume of processes, key risks and controls need to be identified and relevant evidence of the control check should be provided for each material report.

Examples of controls include:

- Documentation of the risk report production processes which clarifies the inputs/outputs as well as the roles and responsibilities of participants.
- Approval of risk reports by report owners and stewards prior to distribution to committee members.

#### 2.4.1.1 Ensure that limitations reports accompany risk reports

Report consumers must be made fully aware of and understand limitations within the risk information that is contained in their risk reports. The Risk Data Aggregation and Risk Reporting Limitations Standard defines the minimum requirements for reporting on limitations, and establishes the required limitations reporting process, roles and responsibilities and governance structures.

#### 2.4.1.2 Review BAU reports annually

The report owners are accountable, and report stewards are responsible for reviewing the scope, quality, frequency, production process and distribution requirements of risk reports with accountable executives. This review must be performed annually or as events may determine.

Report consumers are responsible for ascertaining, defining and reviewing whether or not the information in risk reports meets their information needs regarding content, format, timing and frequency and providing annual feedback (or as events may determine) to producers.

They are to take responsibility for the scope, quality, and distribution requirements of their risk reports and ensure that end user requirements and feedback are taken into consideration. This may be done through periodic meetings or other means, as appropriate.

#### 2.4.2 Implement quality controls

As the Board and risk executive and management committees rely on risk information to make risk decisions, it must be of suitable quality as defined by accountable executives. Controls have a vital role to play in making sure that it does.

Examples of controls include:

- Data quality controls are in place to ensure risk management reports are accurate and measured against data tolerance levels.
- Reconciliation controls (e.g. between risk and finance data) are established to reconcile to risk data used in risk reports and performed in accordance with the reporting cycle and timelines. Reconciling items outside established thresholds were documented, monitored, reported/escalated until remediation.
- Any adjustments raised were approved, monitored and reported in accordance with materiality thresholds and escalation requirements.
- Reasonability checks (e.g. validation rules and movement analysis) and exception reports were established for identifying, reporting and explaining material data errors and weaknesses in data integrity

##### 2.4.2.1 Apply data controls to risk reporting

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

- Report owners are accountable and report stewards responsible for reviewing their documentation whenever they create risk information and updating it as required, ensuring that they accurately represent the risk information production process.
- Report owners and stewards must conduct an annual qualitative assessment on adaptability of risk reports and their ability to respond adequately to OOC report requests.
- Report consumers are responsible for ensuring that risk reports provided meet their quality expectations. At a minimum, this entails ensuring that an accountable executive has attested to its quality and undertake appropriate quality checks.

##### 2.4.2.2 Perform commentary and commentary presentation checks

Report owners are accountable and report stewards responsible for ensuring that checks are conducted on commentary to ensure consistency, accuracy, relevance and timeliness.

#### 2.4.3 Combined Assurance controls

The accountable executive or delegate may from time to time commission the relevant quality assurance team from within the three lines of defence to review risk information production processes and the effectiveness of associated controls as per the Assurance Standard.

## 3. STANDARD GOVERNANCE

## 3.1 Roles and responsibilities

Key roles and responsibilities to achieve the Standard requirements:

| ROLE | RESPONSIBILITY |
|---|---|
| Board risk management committees | • Oversee executive management's ownership and implementation of risk data aggregation and risk reporting principles.<br>• Review the risk reporting requirements most suitable for the size, nature and complexity of the bank's operations.<br>• Approve risk metrics and dimensions as specified in the principal risk frameworks and related policies.<br>• 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.<br>• 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. |
| Executive risk management committees | • Own the implementation and management of risk data aggregation and risk reporting principles.<br>• Define the risk reporting requirements most suitable for the size, nature and complexity of the bank's operations.<br>• Propose the risk metrics and dimensions as specified in the principal risk frameworks and related policies.<br>• 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.<br>• Own the limitations of risk data aggregation affecting the Board risk reports, as per the Risk Data Aggregation and Risk Reporting Limitations Standard. |
| Group Chief Risk Officer (GCRO) | • Accountable for the enterprise wide management of risk data aggregation capabilities and risk reporting processes.<br>• Recommend the scope of risk metrics to be included in risk reporting, to the Board for approval.<br>• Rationalise, plan for and implement the automation of relevant manual activities, in conjunction with the data owners, for enterprise aggregated risk metrics.<br>• Nominate the RRC to address an OOC risk report request, constitute a RRWG if necessary together with the RRC. |
| Principal Risk Officer (PRO) | • Accountable for RDARR for the risk type.<br>• Responsible for implementing the Risk Reporting Standard within the risk type, supported by the Head of Risk Reporting.<br>• Accountable for implementing limitations reporting as per the Risk Data Aggregation and Risk Reporting Limitations Standard.<br>• Accountable for the communication and resolution of limitations relevant to the risk type as per the Risk Data Aggregation and Risk Reporting Limitations Standard. |
| Business Area Chief Risk Officer (BA-CRO) | • Accountable for RDARR for the BA.<br>• Responsible for implementing the Risk Reporting Standard within the BA. |
| Report Owner | • Accountable for maintaining a register of report users, and reviewing this list annually. |

| ROLE | RESPONSIBILITY |
|---|---|
| | • Accountable for ensuring that the scope, quality, timeliness, frequency and distribution requirements of the risk reports are reviewed with users at least annually.<br>• Conduct an annual qualitative assessment on adaptability of risk data to respond to:<br>– Ad hoc requests for risk reporting received during the prior period; and<br>– Requests to make amendments to normal reporting in a timely manner.<br>• Accountable for ensuring that the above controls are also implemented on the risk reporting processes.<br>• Assess new/changed reports against initial requirements and risk information production process & signs-off on final report or requests further development.<br>• Provide annual attestations as to the quality of the reports they are accountable for and keep a record of these attestations and submit those attestations to Enterprise Risk Reporting .<br>• Accountable for assessing report commentary meet consistency, accuracy and applicability criterion. |
| Report Steward | • Responsible for maintaining a register of report users, and reviewing this list annually.<br>• Responsible for ensuring that the scope, quality, timeliness, frequency and distribution requirements of the risk reports are reviewed with users at least annually.<br>• Conduct an annual qualitative assessment on the adaptability of risk data to respond to:<br>– Ad hoc requests for risk reporting received during the prior period; and<br>– Requests to make amendments to normal reporting in a timely manner.<br>• Responsible for ensuring that the above controls are also implemented on the risk reporting processes.<br>• Make sure requirements for new reports are fully documented.<br>• Responsible for assessing new/changed reports against initial requirements and risk information production process and facilitates further required development. |

## 3.2 Adherence

This Standards provisions / control requirements are mandatory for all legal entities and business units as defined as in scope and are used to set a group-wide standard to reporting on risk appetite. The Standard's provisions / control requirements will be audited as such in alignment with the requirements of the related Risk Data Aggregation and Risk Reporting Policy.

Any deviations from the Standard's 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 and, if the trade-off is material, it should be reported to Senior Management and to the Group Risk and Capital Management Committee (GRCMC). The Process Owner is accountable and responsible for assessing the trade-offs. A record of all trade-offs should be maintained.

Non-adherence to any requirement in this Standard 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 to 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 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 in accordance with 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 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 Standard

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

- Enterprise Risk Management Framework
- Entities in Scope for Risk Data Aggregation and Risk Reporting Standard
- Assurance Standard
- Business Continuity Management (BCM) Risk Policy
- Data and Records Management Risk Policy
- End User Developed Applications (EUDA) Standard
- Risk Data Aggregation and Risk Reporting (RDARR) Policy
- Risk Data Aggregation and Risk Reporting Limitations Standard
- Risk and Finance Data Alignment and Reconciliation Standard
- Information Security and Cyber Risk Policy

## 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 |

| Abbreviation / Acronym / Term | Explanation |
|---|---|
| BA-CRO | Business Area Chief Risk Officer |
| BAU | Business As Usual |
| BCBS | Basel Committee on Banking Supervision |
| CDE | Critical Data Element |
| ERMF | Enterprise Risk Management Framework |
| EXCO | Executive Committee |
| GCRO | Group Chief Risk Officer |
| GRCMC | Group Risk and Capital Management Committee |
| IA | Internal Audit |
| OOC | Out of cycle |
| PRO | Principal Risk Officer |
| RDARR | Risk Data Aggregation and Risk Reporting |
| RRC | Risk Reporting Coordinator |
| RRWG | Risk Reporting Working Group |
| SARB | South African Reserve Bank |

### 4.2.2 Definitions

For the purpose of this Standard, the term "Risk Data" is used to incorporate the Data Domains and associated CDEs required for the in-scope risk reporting processes, risk reports and risk metrics.

Within Absa, data is defined in terms of a CDE (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 CDEs e.g. Trade).

| Definition | Explanation |
|---|---|
| Business Area | Retail and Business Bank (RBB), Corporate and Investment Bank (CIB) and Countries are collectively termed BAs. |
| Country and Legal Entity | Countries and Legal Entities falling within the Absa structure. |
| Critical data element (CDE) | CDEs 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 CDEs (e.g. Probability of Default, Risk-Weighted Assets etc.)<br>In the context of the interpretation of this Standard, both risk metrics and risk indicators are deemed critical data. |
| Dimension | An attribute by which a metric is grouped, e.g. legal entity, country code, industry code, etc. |
| Group Function | Operations and Technology, Risk, Finance, Tax, Compliance, Legal, Marketing and Corporate Relations, Treasury, Human Resources and Internal Audit (IA). |

| Definition | Explanation |
|---|---|
| Risk data | The individual data elements (inputs) that are used in the production/ calculation of a risk metric. A risk metric is in itself, risk data. All data used by the Risk function or included in risk reporting, is not automatically classified as "risk data". Non risk metric data is referred to as Risk Management Information. |
| Risk data aggregation | Defining, gathering and processing risk data according to Absa's risk reporting requirements to enable Absa 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.<br>Risk metrics typically take one of three forms:<br>• those that quantify exposure;<br>• those that quantify uncertainty;<br>• those that quantify exposure and uncertainty in some combined manner.<br>*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 |

## 5. RECORD OF VERSION CONTROL / UPDATES

| Date | Author / Source | Change |
|---|---|---|
| 29 August 2019 | Email: Cindy Stringer<br>Circular date: 29 August 2019<br>Circular number: 716/2019 | New Risk Reporting Standard published.<br>• Version 1.0 |
| 22 February 2021 | Email: Cindy Stringer<br>Circular date: 22 February 2021<br>Circular number: 211/2021 | Annual review<br>• Version 2.0 |
| 6 May 2022 | Email: Cindy Stringer<br>Circular date: 6 May 2022<br>Circular number: | Annual review<br>• Version 3.0 |