Santander Holdings USA

Santander

ENTERPRISE

RISK DATA AGGREGATION AND RISK REPORTING FRAMEWORK

Table of Contents

1. Introduction

1.1 Background

Risk Data is essential for SHUSA and its Subsidiaries to achieve their business objectives. To ensure effective data management, data must be subject to defined governance and controls, and clear rules to ensure that it is accurate, timely, consistent and capable of aggregation.

Thus, an effective Risk Data Aggregation and Risk Reporting Framework supports the identification, assessment, control, monitoring, testing and reporting of risks across all risk types and all areas of the business of SHUSA and its Subsidiaries, such as:

- Risk management, monitoring and control; including Data related to internal policies, standards and procedures;
- The setting, reviewing and challenging of risk tolerance;
- Financial decision making;
- Capital, liquidity and funding planning processes;
- Policy changes and transaction assessment;
- Compliance with prevailing regulatory requirements;
- Corporate strategy, mergers, acquisitions and divestitures;
- Business Continuity Plan;
- Data architecture and IT infrastructure strategy;
- Data confidentiality and data security.

1.2 Risk Data Definition

Risk Data is defined as the information required for the sound management and control of all risks and to enable the achievement of SHUSA's business objectives[1].

[1] The data under scope of this Framework does not include local data (i.e. data only used by single user applications and not required to be shared). For example, data manipulated in Excel desktop by an end user for his/her own consumption does not warrant enhanced data management oversight.

This definition includes, but may not be limited to:

- Data managed by SHUSA and its Subsidiaries, or by any vendors that manage data;
- Commercial, corporate, employee and customer information related to products, services, processes, strategies and performance, including risk and financial data as required for Capital Planning and Risk Data aggregation.

1.3 Scope

The Santander Holdings USA, Inc. ("SHUSA" or the "Company") Enterprise Risk Data Aggregation and Reporting Framework ("RDARRF") applies to SHUSA and all its subsidiaries. SHUSA is a U.S. bank holding company with two subsidiaries, Santander Bank, N.A. ("SBNA"), a national bank, and Santander Consumer USA Inc. ("SCUSA"), a public, non-bank consumer finance company that is majority-owned and controlled by SHUSA (together "the organization").

The Company will require that managers at all levels will understand and embed within their organizations the prudent principles described in this Framework.

1.4 Purpose of the Enterprise Risk Data Aggregation and Risk Reporting Framework

The Board of SHUSA has approved an overarching Enterprise Risk Management ("ERM") Framework that sets the principles of SHUSA's oversight of risks arising from its business activities and operations and governs its risk management activities. This RDARRF must be read in conjunction with the SHUSA ERM Framework as its purpose is it to develop the ERM program in relation to risk data. This ERM RDARRF describes the Risk Data Aggregation and Reporting principles and governance that must be followed by SHUSA and its Subsidiaries when managing, controlling, aggregating and reporting Risk data and is designed to achieve consistent practices across the organization in compliance with all applicable rules, regulations and guidance.

This RDARRF must also be read in conjunction with the SHUSA Enterprise Data Management Framework ("EDMF") approved by the Board[2] as it develops, specifically for Risk Data[3] Aggregation and Reporting purposes, the principles set out in the EDMF for the management, control and mitigation of data risk

[2] The SHUSA EDMF is owned by the Technology and Operations ("T&O") function of SHUSA and is applicable throughout the organization.

[3] Risk Data, in the context of the EDMF, is considered a Data Domain. The roles and responsibilities with regards to Risk Data that are reflected in this RDARRF are aligned to the obligations defined in the EDMF for Data Domain owners and Data users.

across the organization in a comprehensive, consistent and effective fashion through the formalization and standardization of the processes, roles and systems that impact data.

The implementation and embedding of the principles defined in this RDARRF will ensure that:

- Risk data is correctly processed throughout its life cycle; from origination, transformation, supply and storage up to the use of data for management and reporting purposes;
- There is homogeneity and consistency of data definitions and data taxonomy between activities, risk types and business areas throughout SHUSA and its Subsidiaries, enabling the assessment of all exposures at an individual and a consolidated level, and including the reporting requirements of Santander, S.A. as SHUSA's shareholder and parent company ("Santander Group" or "Group").
- Continuous improvement of data quality is embedded in the day to day activities through establishing adequate control processes and quality indicators and through the development and maintenance of a robust IT systems infrastructure;
- Roles, responsibilities and processes relating to risk data, including ownership and data quality, are clear and coordinated;
- Standards and procedures are in place for the use, development and management of risk data.

This RDARRF is aligned to the Risk Data Framework and the Risk Reporting, Information and Data Governance Model approved by the Board of Directors of Banco Santander S.A. that establish the principles that must be followed by all Santander Group Subsidiaries when managing Risk Data.

1.5 Document Ownership and Maintenance

As owner, the SHUSA Chief Risk Officer (CRO) is responsible for the development and maintenance of this Framework. The Deputy Chief Risk Officer has primary responsibility for ensuring it is implemented and embedded on a day to day basis.

The RDARRF is approved by the SHUSA Risk Committee ("RC") under recommendation from the SHUSA Enterprise Risk Management Committee ("ERMC")[4].

The Framework must be reviewed at least annually and updated as necessary in the event of material changes to the way SHUSA or its Subsidiaries manage Risk Data, its aggregation or reporting. Material changes, relating to the way risk data is collected, managed and controlled, will be approved by the RC. Non-material changes, such as changes to committee names or clarifications to the Framework contents will be approved by the CRO and noted at ERMC and RC.

[4] For additional information about these committees, refer to section 3.12 of this Framework

2. Risk Data Principles

The following are the SHUSA Risk Data principles, applicable to SHUSA and its Subsidiaries when managing Risk Data:

- **Accountability** – Accountability for Risk Data must be clear and documented:
  - The Board of Directors is ultimately responsible for ensuring the application of this RDARRF;
  - Appropriate and adequate governance will be in place for decisions relating to Risk Data and any changes to key responsibilities or processes;
  - Delegated authority for decisions relating to Risk Data need to be documented, communicated, understood, compliant and effective.
- **Data Definition** – Data needs to be defined correctly and consistently:
  - A Data Dictionary will be in place, aligned to the Santander Group Data Dictionary and regulatory requirements;
  - The Data Dictionary will cover reports, metrics and data concepts as well as their attributes;
  - The Data Dictionary will meet the needs of key data and report owners, must be comprehensive, communicated, understood, complied with, and effective and updated on a regular basis, at least annually.
- **Comprehensive, Detailed, Static and Dynamic** – Data needs to be comprehensive, detailed, static and dynamic:
  - Data will cover all material risks, including those that are off-balance sheet, and be sufficiently detailed to allow such risks to be appropriately identified, assessed, controlled, monitored, tested and reported;
  - Data will be static/historic and dynamic/forward looking, to provide early warnings of any potential breaches of risk limits that may exceed SHUSA’s risk appetite.
- **Flexible, Adaptable and Available on time** – Risk Data needs to be flexible, adaptable and available:
  - Risk data will be timely and available when required. Reporting requirements need to be flexible and adaptable to business demands and regulatory requirements;

  - Standard metrics will be agreed for reporting requirements by all material risk types. Risk reports need to be provided in the agreed format and on time;

  - Risk systems will be capable of producing aggregated risk data promptly for all critical risks[5] during times of stress or crisis.

- **Consistent and Capable of Aggregation** – Risk Data needs to be consistent and capable of aggregation in all aspects including segmentation, granularity and processing:

  - Risk data will be available by Business Line, legal entity, asset type, industry, region and other groupings, as relevant for the risk in question;

  - Risk Data will reconcile with Finance, Accounting and other relevant source data;

  - The Data to be aggregated will be managed in line with agreed SHUSA and Santander Group requirements.

- **Data Quality** – Data will be correct and precise, and of the appropriate quality:

  - Standards will be set for data quality and quality indicators put in place to track quality at all key points of the data life cycle;

  - Controls will be as stringent as those used in accounting and must be automated wherever possible to perform cross checks and minimize errors on data entry;

  - Staff entering data in systems will be adequately trained and informed of data entry requirements;

  - Automatic control mechanisms will be put in place to minimize errors in critical data entry;

  - Control indicators and mechanisms will be put in place to monitor quality of source data;

  - Appropriate and adequate data controls will be in place where third parties are used particularly relating to data entry, and in line with the Supplier Risk Management policy;

  - Information repositories will comply with the required quality criteria and processes;

[5] Critical risks: aggregated credit risk exposure to large corporate borrowers, counterparty credit risk exposures such as derivatives, trading exposures, positions, operating limits and market concentrations by industry and region; liquidity risk indicators such as cash flow /settlements and funding; operational risk indicators that are time-critical

  - Data flows and processing will be clearly traced to their source.

- **Security** – Data will be secure in line with agreed Information Security standards and requirements.

- **Resources and Infrastructure** - Resources and Data infrastructure will be appropriate for the needs of the business:

  - Data systems will support compliance with the principles set out in this framework;

  - Adequate resources will be in place to meet these principles.

- **Documentation** – Appropriate documentation will be in place, and reviewed at least annually:

  - Documentation will include, but is not limited to: Data aggregation and risk report generation policy and procedures; Reconciliation procedures; Policies and procedures for the use and management of data; Data security, confidentiality and data usage policies; Third Party Supplier standards/service agreements regarding data processing and quality.

- **Independent Review** - Risk Data principles and processes, including, but not limited to extraction of data and data aggregation, will be reviewed independently on a regular basis to provide assurance that internal and regulatory requirements are met. The RC must be informed of the results of these reviews and of the on-going monitoring of the quality indicators.

3. SHUSA Risk Data Roles and Responsibilities

3.1 SHUSA Ownership Structure

SHUSA is wholly owned by Banco Santander, S.A. SHUSA is required to meet all its obligations as a U.S. bank holding company, while also harmonizing its policies to the principles approved by the Santander Group Board. To support Santander S.A. in meeting its regulatory obligations, SHUSA will report Risk Data to Santander S.A.

3.2 The SHUSA Board of Directors

The SHUSA Board has overall responsibility for Risk Data. The RC assists the Board to discharge its responsibilities relating to risk data management and control.

With respect to the governance, implementation, and monitoring of the RDARRF, the SHUSA Board has delegated its responsibilities to the SHUSA RC that will review and approve the RDARRF and any related Policies, oversee the implementation of the RDARRF and monitor compliance with the Policies.

3.3 The Chief Executive Officer (“CEO”)

The Board delegates full oversight responsibility to the SHUSA Chief Executive Officer (CEO) for the execution of the business strategy and the management of risk, including Risk Data on a day-to-day basis.

3.4 The Chief Risk Officer (“CRO”)

The SHUSA CRO is an independent executive that reports to the SHUSA RC and the SHUSA CEO.

With regards to Risk Data Aggregation and Reporting, the CRO delegates the day to day oversight of his responsibilities to the Deputy Chief Risk Officer (Deputy CRO), who is supported by the Risk Management Information function that report into this Executive. The CRO’s main responsibilities with regards to Risk Data include:

- Ownership and implementation of the RDARRF;

- Ownership and stewardship of the Risk Data Domain[6];
- Definition and documenting of Risk Data Management and Control Requirements;
- Development and distribution of risk reports with a consistent structure, format and presentation of data;
- Ensuring data used in risk reporting is accurate, precise, consistent and meets agreed quality standards;
- Assurance that the architecture and infrastructure provide adequate support for monitoring, oversight and control of risks relating to risk data;
- Executive sponsorship of the Risk Data Aggregation and Risk Reporting program/project;
- Ensuring regulatory requirements regarding Risk Data Aggregation and Risk Reporting are met;
- Definition of the thresholds to be controlled in data quality standards and establishment and verification of the compliance and certification criteria for Risk Data.

3.5 The Head of Risk Management Information ("Risk MI")

Reporting to the Deputy CRO, the Head of Risk MI's main responsibilities with regards to Risk Data Aggregation and Reporting are to:

- Define the target operating model for the Risk MI organizational structure;
- Define and implement a common approach for gathering risk data and business requirements across the different risk areas, serving as the central point of contact between Risk and CDO, T&O and Finance for all matters related to risk data aggregation and reporting;
- Define the target risk control architecture to support risk to support the business requirements defined by the risk team, in coordination with T&O and Finance;
- Develop risk data aggregation procedures and monitoring mechanisms in coordination with the Risk Management reporting groups;

[6] The domain of data within the responsibility of a Data Owner or Data Steward on to which they apply designated rights and responsibilities. A Data Domain could encompass an entire subject area (e.g. Risk Data) or a specific set of data elements (e.g. Credit Risk Data).

- Define the risk data domain and assign data owners and stewards for each risk data sub-domains (i.e. market, ALM, liquidity, credit, operational, compliance, etc.);

- Ensure a holistic approach to the four components of data management within the risk data domain, and coordinating the different risk data owners: data quality management, data architecture and management, metadata management, data lifecycle and controls;

- Ensure the adequate capture of data at source, so that it is complete, verifiable, correct and in compliance with agreed policies and procedures for the risk data domain;

- Coordinate the identification of the metrics and dimensions needed for risk management and control;

- Establish the data strategy, priorities and goals for data within the risk data domain, in coordination with the risk data owners;

- Coordinate business definitions of data and metadata, and approving the selection of KDEs[7] within the risk data domain with the risk data owners;

- Approve business rules for data quality management within the risk data domain;

- Sponsor and authorize new data initiatives and related projects, including those related to data quality improvements and data quality remediation within the risk data domain;

- Review standards for data within the risk data domain;

- Approve the official sources for data within the risk data domain;

- Authorize access to the risk data under their responsibility;

- Compliance with the RDARRF principles;

- Monitor quality assurance and consistency in the data aggregation practices through annual attestation with Risk Management reporting groups;

- Act as the main point of contact for Risk Management reporting groups to raise and resolve issues pertaining to risk data, risk data aggregation and risk reporting;

- Provide ongoing feedback and support on the framework and risk reporting standards.

[7] Key Data Element (equivalent to CDE or Critical Data Element)

3.6 The Chief Finance Officer ("CFO")

The SHUSA CFO reports to the SHUSA CEO.

With regards to Risk Data Aggregation and Reporting, and working with the CRO, the CFO's main responsibilities are the definition, development and execution of all risk data reporting related to capital adequacy, regulatory capital, asset and liability management, liquidity risk, financial performance and stress-testing results.

3.7 The Managing Director, Technology & Operations ("MD T&O")

The MD T&O is responsible for the SHUSA Enterprise Data Management and Oversight function. He delegates the day to day responsibilities related to data quality to the Chief Data Officer ("CDO") as appropriate. The MD T&O shall:

- Ensure the conceptual consistency of the agreed definitions for risk data and other data fields within the organization;
- Ensure data quality standards related to precision, integrity, consistency and promptness are met through establishing adequate and appropriate control mechanisms in the data aggregation process;
- Ensure data integrity during the entire data extraction and upload process, by means of reconciliation processes;
- Ensure the availability, traceability and quality of data needed for risk data in the terms defined by the risk data function;
- Ensure and checking that all data needs are included in the data repositories in terms of completeness, granularity and availability, and that these are documented in policies and procedures;
- Ensure critical data meets all quality standards and oversees that appropriate mechanisms are in place to identify and correct failures in data entry and maintenance;
- Ensure the minimum business and regulatory technological requirements required for risk data aggregation and reporting are in place;
- Ensure the design, development and execution of all stages of the technological risk data structure, is in line with the agreed criteria and specifications;

- Ensure that technological systems and databases have adequate capacity, availability and operational resilience for the agreed business and regulatory demands of data aggregation and reporting;

- Ensure the development and maintenance of information systems, including the supply, storage and exploitation of information, and the execution of the traceability of the concepts defined from the data source to the information repositories and how they are accessed.

3.8 The Chief Data Officer ("CDO")

Reporting to the MD T&O, the CDO is responsible for ensuring compliance with the Enterprise Data Management Framework (EDMF) and associated policies on a day to day basis. The CDO shall:

- Define and sponsor a program to identify key data management elements, assess effectiveness of control/mitigation environment, monitoring and quality strategies and initiatives, ensuring the roles and responsibilities of all functions across the organization are defined and aligned to the EDRF and RDARRF principles, methodology and policies;

- Safeguard the clarity and consistency of the definitions of metrics, dimensions and concepts performed by the users in each area and ensuring they are adequately understood by the associated technology and operations functions;

- Ensure the identification of the traceability between the metrics, dimensions, concepts, and metadata[8] to the Golden Source[9] and from the Golden Source to the source systems (suppliers) and their documentation in the data dictionary;

- Ensure consistency between the data repositories and in the data supply process from source systems to the different data repositories;

- Transpose the defined metrics, dimensions and concepts to the data dictionary, ensuring compliance with the agreed attributes;

- Ensure the development, maintenance and updating of the data dictionary;

[8] Metadata: the data or information that describes data (i.e. "data about data") and includes aspects such as definitions, owners, official source of data, data models, lineage, and data quality KPIs. Categories of Metadata include, but are not limited to, Business, Technical and Operational.

[9] The "Golden Source" provides a single source and repository of data and information for risk management and control within a particular area or data domain. The repositories contain information which is integrated, related, validated, reconciled with accounting and quality information, with the highest level of available granularity and with sufficient historical depth to be analyzed.

- Review the agreed quality metrics and control dashboards;
- Ensure the completeness of data quality plans associated with the data considered to be critical and monitoring progress against such plans;
- Manage and control the data validation process and certifying compliance with the principles set out in the RDARRF throughout the entire life cycle of the data and reporting;
- Ensure compliance with the agreed risk reporting, information and data governance.

3.9 Risk Data Owners

The Risk MI team shall identify Risk Data Owners for each Risk Data sub-domain[10].

The Risk Data Owner will:

- Ensure a holistic approach to the four components of data management: data quality management, data architecture and management, metadata management, data lifecycle and controls;
- Ensure the adequate capture of data at source, so that it is complete, verifiable, correct and in compliance with agreed policies and procedures;
- The clear identification of the metrics and dimensions needed for risk management and control;
- Establish the data strategy, priorities and goals for data within their Domain;
- Establish business definitions of data and metadata, and approving the selection of KDEs[11] within their Domain;
- Approve business rules for Data quality management within their Domain;
- Sponsor and authorize new Data initiatives and related projects, including those related to data quality improvements and data quality remediation;
- Review standards for data within their Domain;
- Approve the official sources for data within their Domain;
- Authorize access to the risk data under their responsibility;

[10] The Risk MI Function is responsible for defining its data domains and assigning data owners and stewards.

[11] Key Data Element (equivalent to CDE or Critical Data Element)

- Compliance with the RDARRF principles.

The Data Owner may delegate the day to day management of risk data to a Data Steward who will be a subject matter expert in the particular area under ownership.

For data where there is no clear single owner (such as data acquired or needed by multiple processes, e.g. Customer) a group of Owners may be established to develop definitions and standards regarding that common data. The Data Governance Council[12] will review and approve the recommendations of such an Owner Group and adjudicate on issues of contention.

3.10 Report Owner

The Report Owner is defined as each one of the functions in charge of defining the risk reports. The Report Owners will:

- Define the reports required for its information area and the metrics that are to be incorporated by the CDO into the Data Dictionary;
- Determine reporting business requirements and translating them into requirements that the Director T&O can deliver for systems and processes;
- Define the quality standards of the reporting information and safeguard its compliance;
- Generate the reports monitoring the completeness and quality of the content;
- Govern access to reports, ensuring that the recipients of the reports are as agreed;
- Gain and act upon feedback from recipients and users of the report;
- Document the data reporting and exploitation processes;
- Compliance with the RDARRF principles.

3.11 Golden Source Owner

The Golden Source owner is defined as each one of the functions in charge of defining and managing the data model of the information repositories in their respective areas. The Golden Source owners shall:

- Define the metrics, dimensions and concepts included in the repository;

[12] The governance committees for risk data are defined in section 3.12

- Ensure the consistency and quality of the data within the Golden Source;
- Ensure data in the Golden Source is reconciled;
- Evaluate the criticality of the data;
- Review and approve the quality indicators, previously validated by the Chief Data Officer, and proposing tolerance limits;
- Identify the best source of data included in Golden Source;
- Ensure the information is available and accessible to users;
- Compliance with the RDARRF principles.

3.12 Other Functions

Other functions that are relevant for risk data are defined in the SHUSA Enterprise Data Management Framework.

Their responsibilities include, but are not limited to:

- Ensuring compliance with risk data input and maintenance standards;
- Carrying out the necessary training actions for the correct interpretation and input of data at source, and the data maintenance criteria over the course of time;
- Establishing the control mechanisms to be able to swiftly identify and correct failures in risk data entry and maintenance.

3.13 Internal Audit

Internal Audit shall independently review and test on a regular basis how risk data is managed and controlled in line with this framework.

3.14 Risk Management Committees

3.14.1 The SHUSA Risk Committee ("RC")

The SHUSA RC is established by and reports to the SHUSA Board to support the Board in its oversight responsibilities with respect to all risk-taking and risk management activities and compliance matters. With regards to Risk Data, the RC responsibilities include:

- Review on an ongoing basis, and approve no less frequently than annually, the SHUSA Enterprise RDARRF ensuring that it remains appropriate in light of regulatory requirements and SHUSA's and its Subsidiaries strategic goals;

- Monitor and oversee SHUSA's and its Subsidiaries´ data governance, policies and status of data quality for the risk domains;

- Review and oversee the capability of SHUSA's infrastructure to fulfill the data architecture requirements needed to comply with RDA, CCAR, EPS and other regulations;

- Review and escalate to the Board potential risks that the limitation of IT infrastructure can have on data, the status of key projects and initiatives related to Data Governance, Data Architecture, and Data Quality improvement.

3.14.2 The SHUSA Enterprise Risk Management Committee ("ERMC")

The ERMC is a management committee established under the authority of the RC. It is chaired by the SHUSA CRO and is responsible for the oversight and monitoring of all risk-taking and risk management activities across SHUSA, including oversight of Risk Data.

With regards to Risk Data, its responsibilities include the following:

- Support the RC in the discharge of its responsibilities, by reviewing all relevant documentation and management information before submission, and advising RC on the status of Risk Data;

- Receiving relevant information on Risk Data from the Risk Data Aggregation and Risk Reporting Steering Group.

3.14.3 The SHUSA Risk Management Information and Data Governance Council ("Risk MI & Data Governance Council")

The SHUSA Risk MI and Data Governance Council is the approval body for cross-functional data management concerns and supports the implementation of the Data Management Policy ('Policy") approved by the SHUSA Board. It will advise the SHUSA Chief Risk Officer ("CRO") and Enterprise Risk Management Committee ("ERMC") with respect to the Risk Data and Risk Reporting ("RD&RR") for SHUSA, its subsidiaries and Santander Group entities considered for inclusion as subsidiaries of SHUSA as an intermediate holding company ("IHC Entities"). The Council serves as the escalation point for subordinate risk management information and data management working groups and facilitates communication across them. It tracks progress of the strategic risk management information and data management initiatives across all working groups and addresses risks, issues and outstanding items across them. Its responsibilities are described in its Charter and include, but are not limited to:

- Reviewing and recommending for approval the Enterprise Risk Data Aggregation and Risk Reporting Framework, the glossary of risk metrics and inventory of risk reports, the risk data taxonomy, key data elements, key performance indicators and the risk data quality tolerance levels;

- Ensuring risk data owners are compliant with their roles and responsibilities as described in the Framework.

- Reviewing and approving he processes and procedures to produce the monthly and quarterly reports to be submitted to the SHUSA Risk Committee and the Board, Banco Santander, S.A. and regulatory agencies;

- Reviewing and approving new or existing risk data requirements for local, regulatory or Santander Group reporting;

- Coordinating the strategy of risk data projects across SHUSA and its Subsidiaries, including those that impact CCAR, Risk ID, Data Warehousing and Data Marts;

- Reviewing the RD&RR initiatives, and providing the SHUSA CRO, the ERMC, the RC and the Board with regular assessments of the initiatives, and progress and notification of potential risks and issues related to the to their delivery, escalating issues as needed;

- Making decisions on the best use of resources (including budget, staffing, IT development);

- Reviewing matters escalated from Risk Data working groups or from the Data Governance Council;

- Reviewing the progress of the RD&RR initiatives, assessing benefits and approving the plans, objectives and priority of the remediation activities related to Data used for Risk, Finance, Regulatory Reporting and other purposes;

4. Risk Data Key Processes

The implementation throughout SHUSA and its Subsidiaries of the risk data aggregation and reporting processes described below will ensure that risk data reporting remains accurate, clear and complete and on time, and addresses the information requirements of the recipients and decision-makers within the organization.

4.1 Information Requirement Process

Risk Data requirements need to be identified by the Risk stakeholders, with participation of T&O and CDO, agreed and captured in the in the Data Dictionary[13]. This process includes both the generation of new information required for SHUSA, its Subsidiaries or the Santander Group due to local management requirements or to meet regulatory obligations and any changes required to existing information. This might be for risk management, control or reporting purposes.

Data and Report Owners in any function which requires data for risk management or control must clearly define their needs so that T&O can independently analyze them in order to identify and recommend synergies, and once agreed, initiate the information availability process. All key local and Group stakeholders need to be engaged in the process and confirm their agreement. This will include relevant Business Lines, Business Support or Risk Control Units.

4.2 Information Availability Process

Risk Data needs to be available. The objective of this process is to ensure the Data and Report Owners have the information and data necessary for their requirements as agreed through the above process. The main elements of this process are:

- Identification of business and regulatory information requirements by Data/Report Owners;
- Extraction of data from system of origin by T&O;
- Data converted into requested information by T&O;
- Information stored by T&O in repositories and available for use, via user interface[14].

[13] The use of a logical data modeling process to elicit risk data requirements is considered a best practice. A "logical data model" is defined as follows: A structured representation of business data providing unambiguous understanding of business requirements, and therefore provides a sound basis for developing databases

[14] A user interface over the information repositories allows the user to access the available information through pre-defined reports or via ad-hoc queries.

The T&O team will provide assurance that the process maintains the traceability of the requirements, the data of origin and the stored data at all times. The Data Owner and Data Stewards along with the CDO will also provide assurance that appropriate data reconciliation controls are in place across different points in the process to ensure data quality and reliability.

4.3 Information Generation & Data Aggregation Process

Risk Data needs to be generated and be capable of being aggregated at different levels in order to achieve the required information and reports. The main elements of this process are:

- Working with the relevant stakeholders for SHUSA, its Subsidiaries and the Santander Group, T&O develops and agrees data generation and aggregation criteria, parameters and calculation rules for extracting the data required from internal and external source systems, and for its storage in the information repositories;
- T&O executes the plans in line with requirements, ensuring they deliver as agreed with the stakeholders in respect of what, when, to whom and where, and making use of the agreed user interfaces.

The metrics used in the Senior Management and regulatory reports, or any update thereto, must be validated by the relevant Report Owner and assurance provided at the Risk Data Forum.

4.4 Data Management & Governance Process

Risk Data needs to be managed within appropriate governance, ensuring that any modification or change which arises in the information or the data throughout its life cycle, from its origin, supply and storage, up until its use for risk management and reporting, is subject to the agreed governance and is properly documented.

The events which are subject to governance within the data management and governance process are as follows:

- Modification/definition/removal of a report, a metric, quality objectives or plans and KRIs;
- Inclusion of a metric requiring changes to the information repositories or the supply systems;
- Changes to supply systems with an impact on the construction of risk metrics;
- Changes to data processing.

As defined in the EDMF, the SHUSA CDO will be responsible for the Data Management & Governance process as it relates to the Risk and other Data Domains.

4.5 Data Risk Management Process

Data risk needs to be managed. Data risk is defined as the risk associated with a data quality defect. The aim of the data risk management process is to minimize the impact of quality deficiencies on the use of data. This process is based on an evaluation of the data risk in the different areas of the organization and in establishing mitigation plans which may be used to reduce exposure to this risk type. There are four key aspects to this process:

- Classification of data, by data domain and definition of the associated responsibilities;
- Evaluation and agreement of absolute and relative criticality of data to help define the minimum levels of quality required;
- Measurement of impact/materiality related to the potential secondary risk type impacts of data risk;
- Remediation plans with clear ownership, deliverables and milestones must be developed to address data quality issues.

Remediation plans or risk mitigation actions that are defined in order to address data deficiencies will be led by the Data Owner and will be subject to the governance set out by the CDO and monitored by the Data Governance Council and the relevant Risk Committees and Fora.

4.6 Data Quality Process

Risk Data needs to be of adequate and appropriate quality. The aim of this process is to define and execute controls throughout the information life cycle in order to guarantee data quality.

Quality criteria and control processes are required at the following points of the process:

- Data sources (internal and external) –Data Owners and Data Stewards will lead Data Quality remediation plans for their domains. The plans will be developed in conjunction with and supported by T&O. Responsibility for the execution of the plan will be assigned based on the nature of the remediation required (e.g. business, operations or IT).
- Information repositories are the responsibility of the Data Owner. T&O will support the development and agreement of quality KRIs and tolerance thresholds with all stakeholders;

- Reports – The Report owner defines and gains agreement from relevant stakeholders for the reporting quality standards relating to the information set out in the report;

The quality plans, KRIs and, tolerance thresholds and the reporting quality standards must be reviewed on a regular basis at the Risk Data Forum and the Data Governance Council. The SHUSA CDO, in line with the requirements of the DMF, will be responsible for the Data Quality processes.

4.7 Data Analysis & Usage Process

Risk Data, information and reports need to be easily understood and accessible in time and format to allow for suitable analysis and usage.

- Reports should be customized to meet the needs of the different levels of governance, management and users, providing recipients with the data they require for decision making in a precise, clear and efficient way;

- Users should only be provided with data and reports based on their roles and agreed requirements.

The Risk Data Aggregation and Risk Reporting Steering Committee, the Risk Data Forum, the Risk Data Owners and the Risk Report Owners will be responsible for defining and managing an access and permit system to control and govern user access.

4.8 Risk Reporting Process

Risk reports need to be provided to the relevant parties. The form and the frequency in which data and reports are made available shall depend on the relevance and materiality of the reported risk.

The main elements of this process include:

- Risk report recipients define their information requirements including periodicity and covering all material risk areas within SHUSA;

- Risk reports contain an appropriate balance between quantitative and qualitative information;

- Risk reports are prepared by trained and experienced staff with sufficiently knowledge of the subject matter and who will conduct analysis and validation of contents, including reasonableness checks;

- Information is correct and truthful;

- Risk reports are made available in the agreed structure and format, and on time;
- Risk reports conform to confidentiality and security principles.

The Risk Data Aggregation and Risk Reporting Steering Committee and the Risk Data Forum will be responsible for defining, reviewing and approving the format and content of risk reports.

4.9 Certification Process

The certification process reinforces the personal accountability of all those responsible for ensuring that Risk Data is managed and controlled in line with the RDARRF and its principles, key requirements and responsibilities. The RDA certification process is the responsibility of the CDO. The Risk MI function will be responsible for ensuring that all Risk stakeholders perform the certification process in a timely manner. The CDO will ensure the appropriate T&O stakeholders are involved in the certification process.

The main elements of the process include:

- Review of compliance with the key principles, responsibilities, process and governance;
- Analysis, assessment and recommendation of remedial action required, by whom and within what timescale;
- Agreement of remedial action plans, ownership and timescales;
- Tracking and reporting progress against agreed plans.

The status of implementation of the RDARRF must be reviewed on a regular basis at the Risk Data Forum and the Risk Data Aggregation Steering Committee. The self-certification process is a critical input to this review.

4.10 Risk Systems Development Process

Risk Data and its associated systems and processes are in need of constant development and updating in line with changes in business needs, regulatory requirements and technology.

The main elements of the process include:

- Identify new risk data requirements due to business needs, regulation and best practices;
- Evolve systems and processes in line with technological developments;

- Identify, understand and apply learnings from incidents and errors;
- Develop and agree proposal for change with all key stakeholders and in line with agreed governance for technology developments;
- Delivery of agreed changes by T&O in line with the requirements of this framework.

Data Owners and Data Stewards will be responsible for identifying the required technological changes to Risk data management and requirements. Requirements will be developed in conjunction with and supported by T&O and the CDO. Responsibility for the execution of the plan will be assigned based on the nature of the remediation required (e.g. business, operations or IT).

5. Data Policies and Regulatory Obligations

5.1 Data Policies and Process and Administrative Documents

Document Type	*Entity and Department*	*Owner*	*Document Title*
ERM Framework	*SHUSA Risk Governance*	*SHUSA Director, Risk Governance*	*ERM Risk Data Aggregation and Risk Reporting Framework*
ERM Framework	*T&O*	*Chief Data Officer*	*SHUSA Enterprise Data Management Framework*
ERM Policy	*T&O*	*Chief Data Officer*	*SHUSA Enterprise Data Management Policy*

Regulatory Agency/Act	*Citation*	*Title*
Basel Committee on Banking Supervision	*N/A*	*Principles for effective risk data aggregation and risk reporting*

6. Document History and Version Control

1.1 Ownership and Authorship

Version	**Date**	**Author**	**Owner**	**Change**
1.0	August 2015	SHUSA, Head of Risk MI	SHUSA CRO	New Enterprise Risk Data Aggregation and Risk Reporting Framework

1.2 Sign-Off

Approving Body	**Governance Committee Approval or Endorsement**	**Final Approval Date**
SHUSA Risk Committee	Enterprise Risk Management Committee	September 24, 2015