Santander Holdings USA, Inc.

ENTERPRISE MODEL RISK MANAGEMENT POLICY

Santander Holdings USA, Inc. ("SHUSA") believes that our success is grounded in our values, which are also shared by Banco Santander, S.A. and its subsidiaries (collectively with SHUSA, "Santander"). Santander's commitment to treat customers, colleagues and stakeholders in a manner that is *Simple, Personal and Fair* means that every action undertaken by a SHUSA Team Member is founded on *INTEGRITY, CUSTOMER COMMITMENT, PEOPLE, TEAMWORK, OWNERSHIP,* and *INNOVATION*. It is because of this commitment throughout the Santander organization that Santander's customers, clients, and shareholders trust us to deliver world class products and services and select Santander. Safeguarding this trust – by always conducting business responsibly, with integrity and a disciplined approach to risk management – is a responsibility shared by each SHUSA Team Member.

Table of Contents

1 Introduction

1.1 Purpose of the Document

Santander Holdings USA, Inc. ("SHUSA")[1] uses models to support decision making, financial and regulatory reporting, and to provide predictive information in a number of business areas, such as credit risk management, market risk management, capital estimation and stress testing, and asset/liability management, among others.

SHUSA recognizes the potential risks associated with its use of models, as well as the importance of establishing an appropriate program for managing those risks. The purpose of the Enterprise Model Risk Management Policy (the "Policy") is to set out a comprehensive approach to managing model risk throughout SHUSA.

The Policy is aligned with the SHUSA Enterprise Model Risk Management Framework (the "Framework") and is consistent with the principles of the supervisory guidance on model risk management (OCC 2011-12/SR 11-7).

1.2 Scope

The Policy applies to SHUSA. Mirroring the governance structure of SHUSA, SHUSA Operating Entities ("SHUSA OEs") are required to adopt the Policy and the associated Model Risk Management Standards ("Standards") in their entireties, in accordance with their respective governance processes.[2]

1.3 Policy Approval and Maintenance

The Policy is authored and owned by SHUSA's Chief Model Risk Officer ("CMRO"), under the specific authority of the SHUSA Chief Risk Officer ("SHUSA CRO"), reviewed by SHUSA Model Risk Management Committee ("MRMC"), SHUSA Enterprise Risk Management Committee ("SHUSA ERMC"), SHUSA Risk Committee of the Board ("SHUSA RC"), and approved by SHUSA Board of Directors ("SHUSA Board").

The Policy is reviewed and approved at least annually, or when changes are necessary, to ensure that it remains applicable to SHUSA's strategy and current and planned activities. Ad-hoc Policy reviews can be performed at the discretion of the CMRO. The SHUSA CRO, MRMC, SHUSA ERMC, SHUSA RC, or SHUSA Board may also initiate updates to the Policy in response to changing conditions. All material updates to the Policy require the approval of SHUSA Board.

[1] SHUSA is a subset of all operating entities of Banco Santander, S.A.

[2] The Policy is expected to be adopted by all U.S. OEs of Banco Santander, S.A. that are not part of SHUSA.

1.4 Policy Transition Period

The transition period for compliance with the Policy is defined as follows:

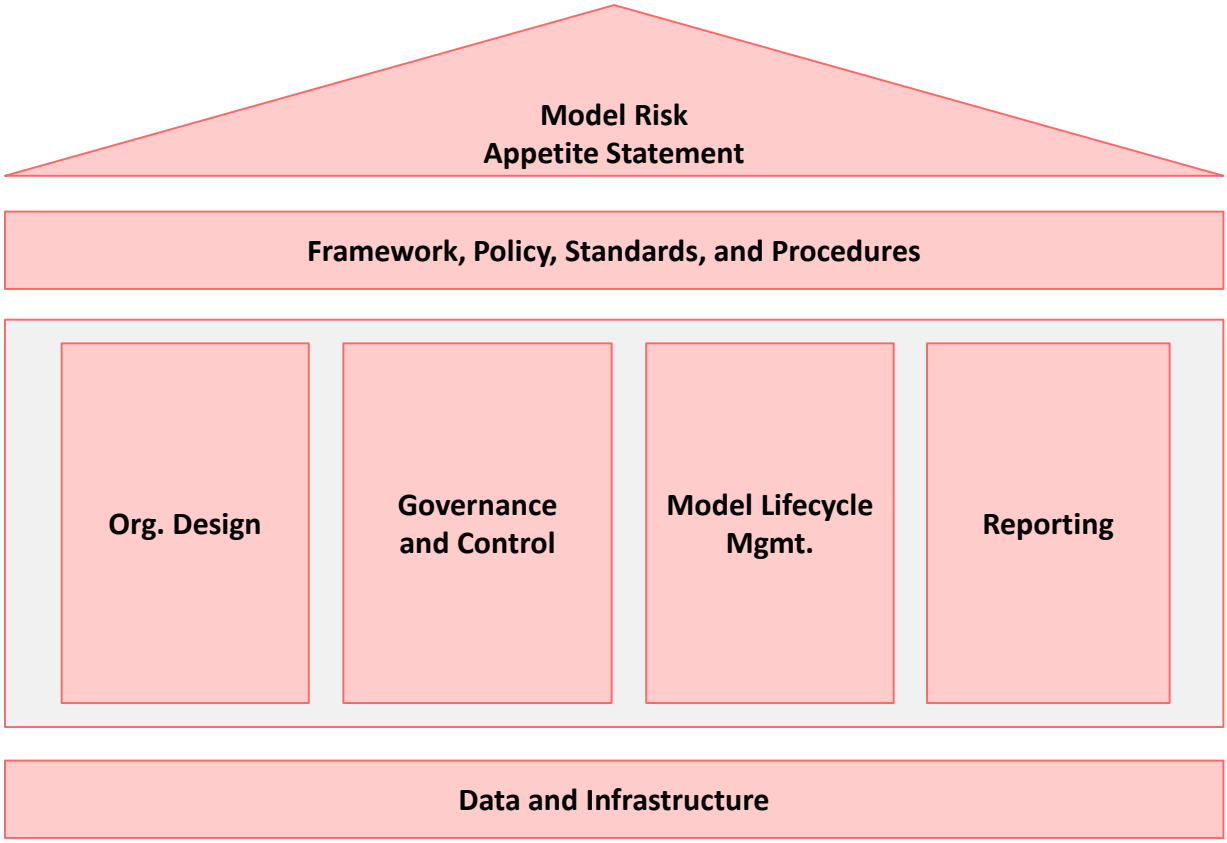
- All new models and major model changes implemented after the final approval date of the Policy must be in full compliance with the Policy
- Legacy Tier 1 models – Tier 1 models, as defined in section 3.5.1, that were in production prior to the effective date of the Policy – must be in compliance with the Policy by December 31, 2017
- All non-Tier 1 legacy models must be in compliance with the Policy by December 31, 2018

1.5 Model Risk Management ("MRM") Operating Model

As detailed in Figure 1 below, the following are the core components of SHUSA's MRM Operating Model:

- **Model Risk Appetite Statement** – Defines the level of model risk acceptable to SHUSA Board
- **Framework, Policy, Standards, and Procedures** – Defines the MRM governance model, functional processes, and roles and responsibilities
- **Organizational Design** – Defines the resource and capability needs for the MRM operating model, as well as the interactional model between the First and Second Lines of Defense
- **Governance and Control** – Ensures effective risk management through adequate escalation processes and senior management accountability
- **Model Lifecycle Management** – Outlines roles and responsibilities across MRM activities throughout the model lifecycle
- **Reporting** – Establishes the model risk monitoring capabilities required to provide effective risk management information to all levels of management for decision making
- **Data and Infrastructure** – Provides the foundation to manage model-related data and information (comprehensive model inventory) to support day-to-day MRM activities

Figure 1: MRM Operating Model



The MRM Operating Model is intended to ensure compliance of SHUSA's MRM activities with regulatory requirements.

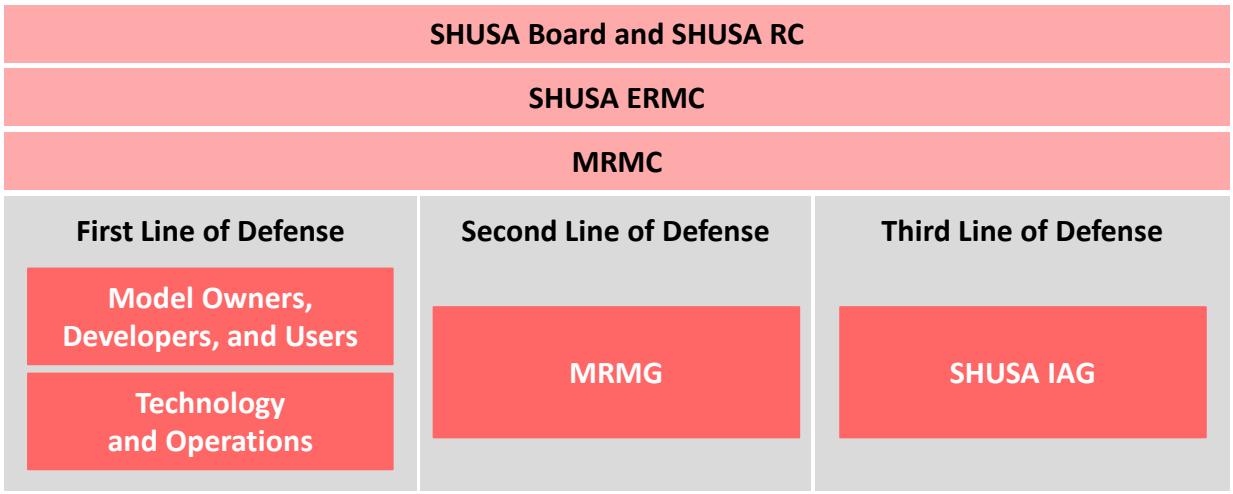
2 Governance and Accountability

SHUSA has established a clear governance structure in line with SHUSA Three Lines of Defense principles for risk management to manage model risk across SHUSA and provide adequate oversight across all MRM activities.

2.1 SHUSA Governance

Figure 2 below lays out SHUSA's MRM Governance structure as defined in this document. The First Line of Defense[3], comprised of Model Owners, Developers, Users, and Technology & Operations ("T&O"), jointly develops or acquires, implements, operates, and maintains models and manages model risk on a day-to-day basis according to the Policy and Standards. The Second Line of Defense, the centralized SHUSA Model Risk Management Group ("MRMG"), designs and implements the approach to model risk management. Finally, the Third Line of Defense, the SHUSA Internal Audit Group ("SHUSA IAG"), assesses the appropriateness and effectiveness of SHUSA's approach to model risk management and reviews compliance of the First and Second Lines with the Policy and Standards. SHUSA Board and SHUSA RC are ultimately responsible for the oversight of model risk at SHUSA and may delegate responsibility to SHUSA ERMC and MRMC. All committee charters must reflect the committees' MRM responsibilities.

Figure 2: MRM Governance and Three Lines of Defense

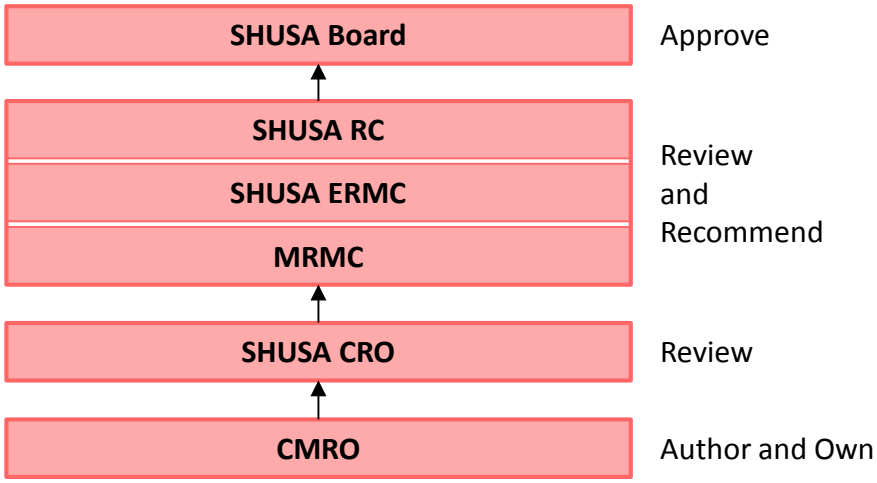


[3] Even though a Model Owner, Developer, or User may be considered to be a part of a Risk organization and represent the Second Line of Defense with respect to other risk types, they would still be considered to be a part of the First Line of Defense with respect to model risk management.

2.2 Policy Governance

The Policy governance structure and responsibilities are outlined below in Figure 3.

Figure 3: SHUSA Policy Governance



2.3 Operating Entity Governance

Each SHUSA OE is required to adopt the Policy and the associated Standards. Each SHUSA OE may supplement the Policy and Standards with amendments or additions that reflect its business and strategy. Any amendments or provisions to the Policy or Standards made by SHUSA OEs must be reviewed and recommended by MRMC to the respective entity's ERMC and RC, as well as approved by the entity's Board.

2.4 Escalation

In the event of a disagreement between MRMG and a Model Owner on the outcome of a validation, the adequacy of a remediation plan, a request to decommission a model, the outcome of an annual review, or an assessment of compliance with the Policy, MRMG must escalate the issue to MRMC to arbitrate. MRMC may involve the relevant Business Area Manager ("BAM") in the arbitration of issues requiring business area expertise. If agreement cannot be reached by MRMC, the issue can be further escalated to SHUSA ERMC for resolution.

2.5 Enforcement

The Policy will be enforced through the application of MRM Compliance Standards, which detail the definition, assessment, and consequences of Policy breaches. Any individual who becomes aware of an instance of non-compliance with the Policy must escalate the issue to the CMRO.

3 Policy

3.1 Policy Statement

SHUSA recognizes that the use of models invariably presents model risk, and is cognizant of the potential for adverse consequences from decisions based on incorrect, inadequate, or misused models. Therefore, SHUSA has established a Policy outlining the principles of model risk management intended to mitigate SHUSA's exposure to model risk.

3.2 Key Definitions

The two key definitions set out below must be used consistently across all MRM-related activities at SHUSA.

3.2.1 Model

For the purpose of the Policy, a "model" is defined as a quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates. A model consists of three components:

- An information input component, which delivers assumptions and data to the model;
- A processing component, which transforms inputs into estimates; and
- A reporting component, which translates the estimates into useful business information.

The definition of a model also covers quantitative approaches whose inputs are partially or wholly qualitative or based on expert judgment, provided that the output is quantitative in nature.

Non-models, which are quantitative or qualitative methods that use deterministic rules to produce exact output values, are not covered under the scope of the Policy.

Models are simplified representations of real-world relationships among observed characteristics, values, and events. Simplification is inevitable but also intentional, to focus attention on particular aspects considered to be most important for a given model application.

Models may be internally developed, developed by a third party, developed by Banco Santander, S.A. or by other entities within SHUSA, or an off-the-shelf vendor system.[4]

Expert judgment models are those approaches that provide outputs that are quantitative in nature, but that do not form a direct linkage with historical data through widely-accepted statistical methods or modeling frameworks. Such approaches may range from the judgmental application of historical data to the use of inputs that are partially or wholly qualitative or based on expert judgment.

[4] Even though a model developed by the parent company or by another entity may have gone through independent validation testing within that entity, SHUSA manages model risk locally in the U.S. in order to ensure compliance with the U.S. Federal Reserve and the Office of the Comptroller Currency ("OCC") regulatory requirements on model risk management.

3.2.2 Model Risk

For the purpose of the Policy, "model risk" is defined as the potential for adverse consequences from decisions based on incorrect, inadequate, or misused model outputs and reports. Model risk can lead to financial loss, poor business and strategic decision making, or damage to SHUSA's reputation. Model risk occurs primarily for two reasons:

- A model may have fundamental errors and may produce inaccurate or inadequate outputs when viewed against the design objective and intended business uses. Errors can occur at any point from design through implementation. In addition, shortcuts, simplifications, or approximations used to manage complicated problems could compromise the integrity and reliability of outputs from those calculations. Finally, the quality of model outputs depends on the quality of input data and assumptions used, and errors in inputs or incorrect assumptions can lead to inaccurate outputs
- A model may be used incorrectly or inappropriately. Even a fundamentally sound model producing accurate outputs consistent with the design objective of the model may exhibit high model risk if it is misapplied or misused

3.3 Model Risk Appetite Statement

SHUSA must create and approve a model risk appetite statement that clearly defines the level of model risk acceptable to SHUSA Board. The model risk appetite statement must incorporate a set of metrics that are intended to facilitate the management and monitoring of key risks, and where appropriate, specific thresholds for these metrics are defined to capture SHUSA's model risk appetite.

Model Owners and BAMs are responsible for ensuring adherence to SHUSA's model risk appetite. MRMG is responsible for reporting to appropriate management and committees to ensure model risk remains within the defined model risk appetite. MRMG is responsible for escalating to MRMC, SHUSA ERMC, and SHUSA RC when actions are required to mitigate excessive risk.

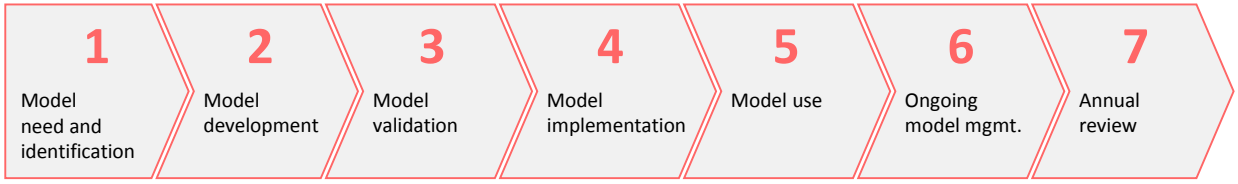
3.4 Model Inventory Management

MRMG must maintain a centralized inventory of all models of all U.S. OEs of Banco Santander, S.A., as defined in section 3.2.1, and their distinct uses. Model inventory management is a key tool in the managing and monitoring of model risk.

3.5 Model Lifecycle

SHUSA recognizes that different types of model risk are present at different stages of a model's lifecycle. SHUSA's model lifecycle management is intended to ensure that appropriate controls are implemented to mitigate model risk across SHUSA. Figure 4 below shows SHUSA's model lifecycle, and the following subsections detail the risk management requirements across the lifecycle components.

Figure 4: Model Lifecycle



3.5.1 Model Need and Identification

Lead Model Developers, Model Owners, Model Users, and MRMG may all identify the need for a new model, for a new model use, or for a model change.

Once the need for a new model or model use is identified, the BAM must confirm the Model Owner. The Model Owner must create a business case for the model prior to initiating development of the new model or validation of the existing model for its new use. Following approval of the business case by the BAM, the Model Owner must provide MRMG the required model information and attributes for the model inventory, including a description of the need for the model or new model use based on the business case. The Model Owner must provide the same information and attributes to MRMG if they are unsure if an item meets the definition of a model in section 3.2.1. MRMG, under the delegated authority of the CMRO, has the ultimate authority to determine whether an item submitted to the inventory is a model or a non-model. Model Owners and BAMs must certify the inventory's completeness and accuracy at least annually.

MRMG must assign each inventoried business use of a model a Risk Tier[5] that reflects the risk associated with the potential impact of model-related issues. For models that expose any U.S. OE of Banco Santander, S.A. to direct financial loss there are three Risk Tiers, 1 through 3, that affect the frequency of periodic revalidation and the nature of ongoing model management activities. Models that do not expose any U.S. OE of Banco Santander, S.A. to direct financial loss are classified as operational models. The table below further defines the Risk Tiers and operational models.

[5] The Model Identification Procedures outline the Risk Tiering methodology and further define Tiers 1 through 3 and operational models.

Model Classification	Definition
Tier 1	A model that covers a large portfolio, is subject to high regulatory scrutiny, is critical for business decision-making, and/or exposes any U.S. OE of Banco Santander, S.A. to significant financial loss
Tier 2	A model that covers a large portfolio, but is subject to less regulatory scrutiny or is less critical for business decision-making; or covers a small portfolio, but is subject to high regulatory scrutiny or is critical for business decision-making
Tier 3	A model that covers a small portfolio, is subject to low regulatory scrutiny, is not critical for business decision-making, and/or exposes any U.S. OE of Banco Santander, S.A.to minimal financial loss
Operational model	A model that does not expose any U.S. OE of Banco Santander, S.A. to direct financial loss

The requirements in the Policy apply to operational models to varying degrees. Operational models are:

- Subject to the model identification requirements in the Policy
- Subject to the development, implementation, use, and ongoing model management requirements in the Policy, with the exception of those that involve interaction with MRMG
- Not subject to the validation and annual review requirements in the Policy

Governance of operational models must be defined as part of the overall governance in the business area that uses them. MRMG has the right to request a validation or review of an operational model at any time.

The Risk Tiering methodology must be transparent, reproducible, documented, and approved by MRMC as part of the Model Identification Procedures. At least annually, Model Owners and MRMG must reassess Risk Tiers for all models in production within the model inventory, including whenever there is a model change or a shift in the internal or external factors that affect a model's risk profile.

Model Owners must define and document business requirements for new models, repurposed models, and changed models. Lead Model Developers must define and document technical requirements for new models, repurposed models, and changed models. MRMG must maintain Model Identification Procedures, which outline the minimum requirements for the model identification process and must be approved by MRMC.

3.5.2 Model Development

Model development involves the design and build of a robust and stable model for a specific use, using a structured and industry-accepted approach, conceptually sound methodologies, mathematically correct coding, accurate and reliable data (internally sourced when possible), and extensive testing. Development methodologies and technical development capabilities must be shared across model developers and MRMG to promote model development best practices.

If the Lead Model Developer or Model Owner decides to develop an expert judgment model, the reason for doing so must be clearly documented and justified with empirical evidence.

3.5.2.1 Development Requirements

Lead Model Developers must adhere to the Model Development Standards during development to better ensure models are appropriate for their intended use.

Data used in development must be relevant and suitable for the model's intended purpose, reliably sourced, and accurate. Model testing must include clearly identified performance metrics, standards for acceptable levels of deviations from targets, and predetermined remediating actions in the event of unacceptable deviations.

For an internally developed model[6], the Lead Model Developer must create comprehensive development documentation that includes a record of all key decisions made throughout the development process and keep this documentation up-to-date. Documentation must be sufficient such that the development process is traceable and can be replicated by someone not associated with the model's development. Documentation must cover the areas required in the Model Development Standards.

For a model that will be implemented on platforms or IT applications other than those on which it was built, the Model Owner must create an implementation plan, which must include details of the testing that will take place as part of implementation and the required accuracy of each test. The Model Owner is responsible for ensuring T&O reviews and agrees on the implementation plan.

For a model that will be implemented on the same platform or IT application on which it was built, the Lead Model Developer must document the operational controls that will be in place.

Model Owners must create a performance and risk monitoring plan for all models. In instances where model performance cannot be monitored, establishing a risk monitoring plan is sufficient.

Model Owners must also document the processes for assumptions management and change management that will be in place for models.

The requirements for model development apply to models developed internally, both by SHUSA resources and by external contractors, and to global models[7]. SHUSA Model Development and Risk Methodology must maintain Model Development Standards, which outline the minimum requirements for model development and must be approved by MRMC.

[6] Internally developed models are models developed within SHUSA.

[7] Global models are models developed by Banco Santander, S.A.

3.5.2.2 Vendor Models

SHUSA Model Development and Risk Methodology is responsible for establishing and maintaining Procedures for the selection and retention of vendor models**.** The Model Owner must document the selection and testing of a vendor model, including the rationale for purchasing a model from a vendor and the evaluation of vendor model options, and must understand and justify any model configuration choices.

Vendor models must meet all identified modeling needs and fulfill, to the extent possible, all requirements applicable to internally developed models. Although replicating development testing conducted by the third party is not required, the Model Owner must ensure that appropriate supplemental testing is performed.

The Model Owner must obtain sufficient model documentation from the vendor to ensure a high level of transparency. The Model Owner must ensure that the model meets minimum documentation and data requirements and employs a model methodology in line with industry practices. Providers of vendor models must have model development standards and adhere to a model development governance structure.

Vendor models must be included in the model inventory and are subject to the requirements of the Policy.

3.5.3 Model Validation

3.5.3.1 Validation Requirements

Model validation refers to the activities and processes that ensure a model is performing as intended, in line with its design objectives and business uses. MRMG, a centralized internal function independent from model development and use, is responsible for validation. MRMG must have the requisite knowledge, skills, expertise, familiarity with the business area, and understanding of the intended use of a model to conduct effective challenge of model development.

Effective model validation must include an assessment of the following aspects of a model:

- Input data – The model development data used to build the model, including its validity and suitability and any expert judgment
- Conceptual soundness – The model's approach, construction, and key assumptions
- Output – The model's outputs and performance, including back-testing, sensitivity analysis, overlays, and overrides
- Implementation and controls – The implementation plan and the operational controls around the model production application and the model's security measures
- Governance and oversight – The performance and risk monitoring plan, change management, business reporting, and additional monitoring activities

There are three types of validation activities that a model may undergo throughout its lifecycle:

- **Baseline validation** is the initial validation for internally developed, global, or vendor models. A full-scope baseline validation is required for Tier 1, 2, and 3 models prior to use
- **Change-based validation** is the validation that must take place following a material change to a model or its use. The depth of validation will vary based on the particular change to the model
- **Periodic revalidation** is the revalidation of models that have already undergone a baseline validation. The frequency of revalidation will depend on MRMG's understanding of the model, its recent performance, and its specific risks. The minimum frequency of revalidation is as follows:

Model Risk tier	Cycle Length
Tier 1	2 years
Tier 2	3 years
Tier 3	4 years

MRMG must classify issues identified during validation into two categories: limitations, which have a limited impact on model output and can only be addressed through redevelopment, and findings, which have a significant impact on the model or can be reasonably remediated by the Model Owner. To inform the prioritization of remediation efforts, MRMG must categorize validation findings according to their severity.

MRMG must maintain Model Validation Standards, which outline the minimum requirements for model validation and must be approved by MRMC.

3.5.3.2 Requirements for Global Models

Global models must adhere to the same validation principles that are applied to internally developed models. The validation of a global model may leverage the results of the validation performed by Banco Santander, S.A., provided the results are reviewed and challenged.

3.5.3.3 Requirements for Vendor Models

Vendor models must adhere to the same validation principles that are applied to internally developed models. The validation process for vendor models must mirror that of internally developed models to the extent possible.

3.5.3.4 Requirements for Expert Judgment Models

All expert judgment models must undergo an effective challenge before use. The effective challenge must be conducted by an oversight forum of subject matter experts who were not involved in the development process. MRMG must ensure that the effective challenge process is conducted in line with any established requirements. MRMG must maintain Expert Judgment Model Standards, which outline the minimum requirements for effective challenge of expert judgment models and must be approved by MRMC.

3.5.3.5 Process Management

A designated internal resource from MRMG must oversee, manage, and evaluate all validations conducted by external resources, and these validations are subject to the same criteria, requirements, and processes as those conducted by internal resources. In addition, MRMG must have a contingency plan in the event external resources are no longer available or deemed unsatisfactory. If an external resource assisted in the development of a model, that external resource cannot participate in the validation of that model or similar models.

3.5.3.6 Validation Outcome

Depending on the nature and severity of model findings identified during validation, the outcome of validation will fall into one of three categories:

- Pass – the model is fit for its intended use
- Pass with Findings – the model is generally fit for its intended use but is approved subject to the condition that its identified deficiencies are resolved within the specified time period
- Fail – the model is not fit for intended use and must be changed to address the critical weaknesses identified. Once remediated, the model must undergo another round of validation

Each model that receives a validation outcome of Pass or Pass with Findings must be assigned a Residual Risk Rating, used to aggregate and report on model risk.

3.5.3.7 Model Approval

Prior to use of a model, the CMRO must approve a model's validation outcome of Pass or Pass with Findings. The CMRO approval must detail the specific use or uses for which the model is approved, the period of time during which the model can be used, and any necessary compensating controls. Model approval must be reconfirmed by the CMRO at least every 12 months during the annual review. For models receiving a validation outcome of Pass with Findings, a remediation plan for remediating findings within a specified time frame must be created by the Model Owner and approved by the CMRO before model use.

3.5.4 Model Implementation

Implementation of a model on a platform or IT application other than that on which it was built must be conducted by T&O in accordance with the implementation plan approved during validation. T&O must conduct functional testing to ensure consistency between the developed methodology and the implemented model, and the Model Owner must conduct user acceptance testing ("UAT") in normal and stressed operating scenarios to ensure that the model's components, data inputs, and calculations in the production environment are processed correctly and that the implemented model is consistent with the Model Owner's needs. The Model Owner must document the results of UAT and provide the results to MRMG before model use. Based on a review of the results of the UAT by MRMG, the CMRO has the right to withdraw a model's approval.

Implementation in the production environment must be documented by T&O and the documentation must be kept-up-to-date for each model and maintained by the Model Owner. Documentation must account for:

- Model production specifications covering the end-to-end process from data inputs extraction to output reporting
- Operational controls around the model, designed to ensure appropriate and correct ongoing use of the model, integrity of the production data, and protection from unauthorized changes and use

Lead Model Developers must implement operational controls and create implementation documentation for models implemented on the same platform or IT application on which they were built.

T&O must maintain Model Implementation Standards, which outline the minimum requirements for model implementation and must be approved by MRMC.

3.5.5 Model Use

Model Users must only use model for their validated and approved uses, with the required compensating controls, and for the approved time period.

The Model Owner must clearly articulate model limitations or restrictions that impact model use to all Model Users. The use of overlays or overrides by a Model User must be transparent; conservative but reasonable; reviewed, challenged, and approved by the appropriate oversight forums[8]; and clearly documented.

Reports used for business decisions must be clear and comprehensible for decision makers. The presentation of model output reports and the supplemental information they contain will vary from model to model and from use to use.

MRMG must maintain Model Use Standards, which outline the minimum requirements for model use and must be approved by MRMC.

3.5.6 Ongoing Model Management

Ongoing Model Management consists of performance and risk monitoring, change management, and model decommissioning.

MRMG must maintain Ongoing Model Management Standards, which outline the minimum requirements for ongoing model management and must be approved by MRMC.

[8] The appropriate oversight forums will differ based on the model type and business area using the model. Each oversight forum's responsibilities with respect to review, challenge, and approval of model overlays and overrides are defined in the forum's charter or statement of purpose.

3.5.6.1 Performance and Risk Monitoring

Model Owners must execute performance and risk monitoring in accordance with the performance and risk monitoring plan approved during validation.

- Performance monitoring must consider, at a minimum, analysis that allows an assessment of the model, including activities such as back testing and other assessments of a model's predictive accuracy
- Risk monitoring must consider, at a minimum, changes to the model, changes to the business profile (e.g., the composition of the portfolio) of any U.S. OE of Banco Santander, S.A., changes to market conditions, and an assessment of the model's weaknesses, limitations, and associated risk mitigants

The Model Owner must report performance and risk monitoring results to key stakeholders, including MRMG, for Tier 1, 2, and 3 models. As part of this reporting, the Model Owner must identify key limitations of the performance and risk monitoring. The frequency and type of performance and risk monitoring, including metrics and thresholds, will vary based on the frequency of model use, availability of new data, and magnitude of the model risk. The Model Owner must categorize issues identified during the monitoring process according to their level of severity, with an escalation and remediation process defined for each level.

3.5.6.2 Change Management

Any model changes not pre-approved as part of validation must receive approval from MRMG before being made by the Model Owner. The Model Owner must log and document, sufficiently test, and communicate to key stakeholders, including MRMG, all model changes well in advance of implementation. If MRMG determines that a change to a model is material, the Model Owner must submit the model for a change-based validation prior to use as detailed in section 3.5.3.

3.5.6.3 Model Decommissioning

Before decommissioning a model, the Model Owner must request and receive CMRO approval, following MRMG's model decommissioning process.

If the Model Owner decides to reactivate a model and the model's approval has not expired, the Model Owner must submit the model to MRMG, which will either require validation or permit the model to be used. If the model's approval has expired, the model must undergo validation prior to use.

3.5.7 Annual Review

All Tier 1, 2, and 3 models are subject to an annual review. MRMG must document the annual review process and outcome.

MRMG must perform reviews, at a minimum, within 12 months from the completion of the most recent annual review or validation. A review may be performed more frequently if warranted by material changes to the model or its use, significant increase in the risk profile of the model as indicated by performance and risk monitoring, or at the discretion of MRMG. For all Tier 1, 2, and 3 models, the annual review consists of a reevaluation of the model's Risk Tier. For Tier 1 and 2 models, MRMG must conduct an additional assessment, which covers at a minimum performance and risk monitoring results, to determine the adequacy of past validation activities given potential changes in model risk.

There are three potential outcomes of the annual review:

1. Confirmation of the model approval
2. Requirement for remediating actions and/or acceleration of the validation schedule
3. Withdrawal of the model's approval

If the annual review results in validation activity, the review also determines the scope of the validation.

4 Roles and Responsibilities

The key roles and responsibilities for the execution of model risk management are defined below.

Model Owner: A sufficiently senior person assigned primary First Line of Defense responsibilities for managing model risk for a specific model or models. A given model must have only one designated Model Owner even when the model has multiple business uses. If, for example, a model has two uses, each with a separate Model Owner, these uses must be inventoried as two distinct models. Model Owners may be located in any U.S. OE of Banco Santander, S.A.

Model Need and Identification

- Identify needs for new model development and communicate them to the respective BAM
- Identify needs for model repurposing and communicate them to the respective BAM
- Create a business case for the model prior to initiating development of a new model or validation of an existing model for a new use
- Inform MRMG of the need for a new model, model repurposing, and model changes and submit the required model information for the inventory
- Define model business requirements prior to the development process
- Determine how to fulfill model need (internal, internal with third party assistance, global, vendor)
- Self-identify Model Owners for internal, vendor, and global models
- Certify that the model inventory information is accurate and up-to-date as part of the annual certification process
- Acknowledge agreement with assigned Risk Tiers

Model Development

- Secure adequate resources for model development
- Oversee and document the vendor model selection process, including testing to demonstrate the adequacy of the model for use
- Ensure adequate documentation for vendor models occurs
- Create a model implementation plan for a model that will be implemented on a platform or IT application other than that on which it was built and obtain T&O agreement as applicable
- Create a performance (where possible) and risk monitoring plan for all models
- Document the assumptions management and change management processes for all models
- Review each model, including its assumptions and conservatism, to ensure that it meets business requirements prior to validation
- Inform MRMG when development will be complete so MRMG can schedule the validation

Model Validation

- Submit complete validation request, including all required data, documentation, and other relevant materials
- Sign-off on validation results
- Create a remediation plan to remediate validation findings and submit it to MRMG for approval for models that receive a Pass with Findings validation outcome
- Execute the approved remediation plan

Model Implementation

- Secure adequate resources for and manage model implementation
- Request changes to the model implementation, if necessary
- Identify and implement robust operational controls prior to formal model use
- Review UAT and submit results to MRMG
- Maintain model implementation documentation

Model Use

- Review model limitations as detailed in the development documentation
- Identify approved Model Users and communicate to them the model's limitations and intended uses
- Ensure model is used in line with intended purpose and approved uses
- Design and ensure adequacy of model output reports

Ongoing Model Management

- Execute ongoing performance and risk monitoring in line with approved performance and risk monitoring plans
- Report performance and risk monitoring results as well as any monitoring issues or shortcomings to all relevant stakeholders at the frequency defined in the approved performance and risk monitoring plans
- Request approval from MRMG of any model changes that were not pre-approved during validation, provide UAT results to MRMG for model changes, and communicate all changes to key stakeholders
- Categorize issues identified during the performance and risk monitoring process according to their level of severity
- Communicate model decommissioning and reactivation to MRMG

Annual Review

- Collect all required documentation and data for the annual review and submit it to MRMG

Lead Model Developer: A sufficiently senior person assigned responsibility for leading the effort to develop a model. Lead Model Developers may be located in any U.S. OE of Banco Santander, S.A.

Model Need and Identification

- Identify needs for new model development and communicate them to the respective BAM
- Identify needs for model repurposing and communicate them to the respective BAM and Model Owner
- Identify needs for model modification and communicate them to the respective Model Owner

Model Development

- Fulfill model development projects in accordance with this Policy, the project business requirements, SHUSA Model Development Standards, and generally-accepted mathematical modeling practices
- Prepare model development plans and documentation for review and challenge by applicable key stakeholders
- Document the operational controls that will be in place for a model implemented on the same platform or IT application on which it was built
- Maintain regular communication with the Model Owner, particularly with respect to the model's methodology, limitations, and any associated risks

Model Validation

- Provide requisite information in support of model validation activities
- Execute the remediation plan for a model that receives a Pass with Findings validation outcome

Model Implementation

- Participate in functional testing
- Implement operational controls and create implementation documentation for a model implemented on the same platform or IT application on which it was built

Model User: The person assigned responsibility for the use of a model for a business purpose. Model Users may be located in any U.S. OE of Banco Santander, S.A.

Model Need and Identification

- Identify needs for new model development and communicate them to the respective BAM
- Identify needs for model repurposing and communicate them to the respective BAM and Model Owner
- Identify needs for model modification and communicate them to the respective Model Owner

Model Use

- Review model limitations, model restrictions, model issues, and approved model uses as listed in the development documentation and validation report prior to production or use

- Review model output reports to ensure accuracy before submitting to relevant stakeholders
- Use model in line with intended purpose and approved uses

SHUSA Model Development and Risk Methodology: The SHUSA unit responsible for supervising the model development program within SHUSA.

Model Development

- Formulate, promulgate, and maintain Model Development Standards, Procedures, and Templates
- Identify needs for new model development and communicate them to the respective BAM
- Identify needs for model repurposing and communicate them to the respective BAM and Model Owner
- Identify needs for model modification and communicate them to the respective Model Owner

T&O: The unit assigned responsibility for implementing models on platforms or IT applications other than those on which they were built

Model Development

- For models implemented on platforms or IT applications other than those on which they were built, review and agree on the implementation plan provided as part of the model documentation

Model Implementation

- For models implemented on platforms or IT applications other than those on which they were built:
  - Implement model and apply robust operational controls in accordance with the approved implementation plan
  - Conduct model implementation testing
  - Create implementation documentation
- Maintain Model Implementation Standards

BAM: A senior manager within each functional or business area assigned the MRM responsibilities listed below by MRMG. BAMs may be located in any U.S. OE of Banco Santander, S.A.

Model Need and Identification

- Provide ongoing oversight in the identification of new models and model uses
- Confirm the Model Owner for a new model or new model use
- Approve a business case for the model prior to the initiation of development of a new model or validation of an existing model for a new use
- Certify the completeness and accuracy of the model inventory for their business area as part of the annual certification process

Business Control Officer ("BCO"): A sufficiently senior member within a business area who ensures risk management activities are carried out in a controlled manner across a business area. BCOs provide quality assurance for the First Line of Defense and act on its behalf to ensure compliance with the Policy and Standards. BCOs may be located in any U.S. OE of Banco Santander, S.A.

Model Need and Identification

- Execute testing program to ensure compliance with the Policy and Standards, including the correctness of the certification process

MRMG: The SHUSA unit assigned responsibility for designing and implementing the approach to model risk management

Model Need and Identification

- Identify the need for a new model, model repurposing, and model changes as a result of the annual review and ongoing model management processes
- Define inventory requirements and maintain a centralized inventory
- Oversee the annual inventory certification process
- Classify computational processes as models or non-models
- Assign and reassess Risk Tiers
- Maintain a sound Model Risk Tiering methodology
- Report significant changes to the overall model inventory distribution by Risk Tier to MRMC
- Maintain Model Identification Procedures

Model Validation

- Schedule validations and inform the Model Owner of the scheduled time
- Conduct independent validation of all models in accordance with the Model Validation Standards and determine a validation outcome
- Oversee and manage all validations conducted by external resources
- Ensure effective challenge of expert judgment models through oversight forums
- Document validation results
- Determine a model's Residual Risk Rating for models that receive a validation outcome of Pass or Pass with Findings
- Review and challenge the results of existing validation efforts for global models
- Track the execution of remediation plans
- Maintain an approach to categorizing findings based on their severity
- Maintain Expert Judgment Model Standards

- Maintain Model Validation Standards and Model Validation and Annual Review Procedures

Model Implementation

- Review the results of UAT

Model Use

- Maintain Model Use Standards

Ongoing Model Management

- Receive and independently review performance and risk monitoring results
- Oversee the change management process, approving model changes and initiating change-based validation as necessary
- Aggregate model risk across all models in the model inventory and report to MRMC, SHUSA ERMC, and SHUSA RC
- Determine whether validation is necessary for reactivated models
- Maintain Ongoing Model Management Standards

Annual Review

- Perform review of Tier 1, 2, and 3 models and determine the scope of follow-up actions
- Notify Model Owner of annual review outcomes and any issues that are identified
- Document annual review process

CMRO: The individual with ownership of the Policy and responsibility for overseeing MRMG and the implementation of the approach to model risk management

Model Validation

- Approve models for use based on the outcome of the independent validation
- Approve remediation plans submitted by Model Owners

Model Implementation

- Determine if there is a need to withdraw the model's approval based on MRMG's review of the UAT

Ongoing Model Management

- Approve remediation plans to address issues identified during performance and risk monitoring
- Approve Model Owners' requests to decommission models

Annual Review

- Approve the outcome of the annual review

MRMC: The committee responsible for providing oversight across all MRM activities and for serving as a point of escalation for MRM issues between the First and Second Lines of Defense

Model Need and Identification

- Approve Model Identification Procedures
- Approve the Risk Tiering methodology

Model Development

- Approve Model Development Standards

Model Validation

- Approve Expert Judgment Model Standards
- Approve Model Validation Standards
- Determine a validation outcome when the CMRO refers an outcome sign-off to MRMC
- Arbitrate disputes between Model Owners and MRMG over the validation outcome, the adequacy of a remediation plan, permission to decommission a model, the annual review outcome, and an assessment of compliance with the Policy
- Enforce the remediation timelines outlined in approved remediation plans
- Approve Provisional Approvals for non-CCAR models[9]
- Approve Revalidation Delays[10]
- Approve Policy Exceptions unrelated to validation

Model Implementation

- Approve Model Implementation Standards

Model Use

- Approve Model Use Standards

Ongoing Model Management

- Approve Ongoing Model Management Standards
- Provide effective challenge and governance based on regular risk reports provided by MRMG

[9] Provisional Approvals detailed in section 6

[10] Revalidation Delays detailed in section 6

SHUSA ERMC: The SHUSA committee responsible for supporting SHUSA RC by supervising all risk types across SHUSA, escalating material issues, and recommending certain foundational risk management documents to SHUSA Board

- Approve MRM Compliance Standards

Model Validation

- Approve Temporary Exceptions[11]
- Approve Provisional Approvals for CCAR models
- Inform SHUSA RC of the decision to approve Temporary Exceptions and Provisional Approvals for CCAR models

SHUSA RC: The SHUSA committee responsible for assisting SHUSA Board in its oversight responsibilities with respect to enterprise risk management activities and related compliance matters

- Provide oversight of model risk at SHUSA and delegate authority to SHUSA ERMC and MRMC

SHUSA Board: The appointed body of individuals responsible for establishing the culture, incentives, structure, and processes necessary to promote compliance with MRM principles and regulatory guidance across SHUSA

- Approve the Policy and all material updates to the Policy

SHUSA IAG: A unit that acts as the Third Line of Defense for model risk management

- Assess the appropriateness and effectiveness of SHUSA's approach to model risk management
- Review compliance of the First and Second Lines with the Policy and Standards

[11] Temporary Exceptions detailed in section 6

5 Reporting Structure

Aggregate model risk reports are designed to assist senior management in monitoring and managing model risk. Aggregate model risk reporting must track key risk indicators to support model risk appetite monitoring and to provide MRMC, SHUSA ERMC, and SHUSA RC with accurate information for decision making, effective oversight, review, and challenge. MRMG is responsible for aggregate model risk reporting. Reporting to MRMC must take place at least on a monthly basis. Reporting to SHUSA ERMC and SHUSA RC must take place at least as often as the respective committee convenes.

MRMG is responsible for reporting on non-compliance with the Policy and Policy Exceptions to MRMC, SHIUSA ERMC, and SHUSA RC.

6 Exceptions

The Policy outlines three specific exceptions related to validations:

- **Temporary Exception** – If a model receives a validation outcome of Fail, but cannot be decommissioned because the output is critical for ongoing business activities and there are no suitable substitutes, the Model Owner may request a Temporary Exception to use the model for a period of no more than 180 days. If the Model Owner requests a Temporary Exception, the Model Owner must also propose risk mitigants or temporary overlays to the model output to compensate for the identified issues. A Temporary Exception may be re-approved only once. SHUSA ERMC determines whether to approve Temporary Exception requests for all models, and must inform SHUSA RC of approvals of Temporary Exception requests for CCAR models
- **Provisional Approval** – If there is insufficient time for a model to undergo a baseline validation, the output is critical for ongoing business activities, and the Model Owner has submitted all of the materials required for validation of the model to MRMG, the Model Owner may request a Provisional Approval to use the model for a period of no more than 180 days. As part of the Provisional Approval process, MRMG must review the model to provide a sufficient initial level of comfort with the model's methodology and approach. The CMRO must provide a recommendation to the relevant approval body. SHUSA ERMC determines whether to approve Provisional Approval requests for CCAR models and must inform SHUSA RC of approvals; MRMC determines whether to approve Provisional Approval requests for non-CCAR models
- **Revalidation Delay** – If a model is scheduled for mandatory revalidation, but either MRMG or the Model Owner determines that there is valid reason for delaying revalidation, the Model Owner may request a Revalidation Delay for a period of no more than 180 days. MRMC determines whether to approve Revalidation Delay requests for all models

All exceptions to the Policy unrelated to validations must be approved by MRMC and escalated to relevant committees as deemed necessary by MRMC.

7 Document History and Version Control

7.1 Ownership and Authorship

Version	Date	Author	Owner	Reason for change
1.0	5/24/2015	MRMG	CMRO	Initial Version
2.0	9/25/2015	CMRO	CMRO	Refresh of current MRM program

7.2 Sign Off

Approving body	Governance committee approval	Final approval date
SHUSA Board	SHUSA RC/SHUSA ERMC/MRMC	9/25/2015

8 Appendices

8.1 Appendix A - Stakeholder Definitions

MRM stakeholders, as recognized in the Policy, are summarized below:

- **Model Owner** – A sufficiently senior person assigned primary First Line of Defense responsibilities for managing model risk for a specific model or models. A given model must have only one designated Model Owner even when the model has multiple business uses. If, for example, a model has two uses, each with a separate Model Owner, these uses must be inventoried as two distinct models. Model Owners may be located in any U.S. OE of Banco Santander, S.A.
- **Lead Model Developer** – A sufficiently senior person assigned responsibility for leading the effort to develop a model. Lead Model Developers may be located in any U.S. OE of Banco Santander, S.A.
- **Model User** – A person assigned responsibility for the use of a model for business purpose. Model Users may be located in any U.S. OE of Banco Santander, S.A.
- **SHUSA Model Development and Risk Methodology** – The SHUSA unit responsible for supervising the model development program within SHUSA
- **Technology and Operations (T&O)** – The unit assigned responsibility for implementing models into their production environment
- **Business Area Manager (BAM)** – A senior manager within each functional or business area assigned MRM responsibilities defined in section 4
- **Business Control Officer (BCO)** – A sufficiently senior member within a business area who ensures proper risk management activities are carried out across a business area. BCOs provide quality assurance for the First Line of Defense and act on its behalf to ensure compliance with the Policy and Standards. BCOs may be located in any U.S. OE of Banco Santander, S.A.
- **Model Risk Management Group (MRMG)** – The SHUSA unit assigned responsibility for designing and implementing the approach to model risk management
- **Model Risk Management Committee (MRMC)** – The committee responsible for providing oversight across all MRM activities and for serving as a point of escalation for MRM issues between the First and Second Lines of Defense
- **SHUSA Enterprise Risk Management Committee (SHUSA ERMC)** – The SHUSA committee responsible for supporting SHUSA RC by supervising all risk types across SHUSA, escalating material issues, and recommending certain foundational risk management documents to SHUSA Board
- **SHUSA Risk Committee of the Board (SHUSA RC)** – The SHUSA committee responsible for assisting SHUSA Board in its oversight responsibilities with respect to enterprise risk management activities and related compliance matters
- **SHUSA Board of Directors (SHUSA Board) –** The appointed body of individuals responsible for establishing the culture, incentives, structure, and processes necessary to promote compliance with MRM principles and regulatory guidance across SHUSA

- **SHUSA Internal Audit Group (IAG)** – The SHUSA unit that acts as the Third Line of Defense for model risk management

8.2 Appendix B - Key Terms

- Annual Review – An annual process that entails a reevaluation of a model's Risk Tier and an assessment to determine the adequacy of past validation activities given potential changes in model risk, including an evaluation of performance and risk monitoring where applicable
- Business Area – A major functional area or line of business
- Compensating Controls – Processes or adjustments designed to account for known limitations or weaknesses in a model
- Certification – An annual process during which Model Owners and BAMs confirm that the model inventory is both complete and accurate for their business areas
- Effective Challenge – A critical analysis by objective, informed parties who can identify model limitations and assumptions and produce appropriate changes
- Expert Judgment – A qualitative assessment based on SHUSA-internal or industry experience of subject matter experts
- Expert Judgment Model – See section 3.2.1 for the definition of an expert judgment model
- Global Model – Models developed by Banco Santander, S.A.
- Model – See section 3.2.1 for the definition of a model
- Model Development – The process of building a model, from the initial definition of model purpose, through the determination of a model development approach, identification of development data, model design and build, and testing
- Model Implementation – The process by which developed model methodology and processing components are transferred to functional computer environments so that they can be deployed for regular use by Model Users
- Model Inventory – The centralized database maintained by MRMG including the full list of models used across all U.S. OEs of Banco Santander, S.A., as well as relevant model attributes and risk factors
- Model Lifecycle – The seven stages in the life of a model as outlined in Figure 4 in section 3.5
- Model Risk – See section 3.2.2 for the definition of model risk
- Model Risk Appetite Statement – A formal statement approved by SHUSA RC which defines the level of model risk SHUSA is willing to undertake
- Model Use – The process of generating model outputs and applying them in business decision-making
- Model Validation – Model integrity activities undertaken by a group that is independent from the group(s) responsible for the development and use of a model
- Ongoing Model Management – Consists of performance and risk monitoring, change management, and model decommissioning
- Operating Entity – A legally defined operating unit

- Operational Model – A model that does not expose any U.S. OE of Banco Santander, S.A. to direct financial loss
- Overlay – Any subjective modification to model output
- Override – Any instance whereby an action recommended by the model output is ignored, altered, or reversed based on the expert judgment of the Model User
- Residual Risk Rating – A numerical scoring system used to risk-rank models in the model inventory, enable targeted MRM activities, enhance reporting of aggregate model risk levels and trends to senior management and oversight forums, and assess aggregate model risk across different OEs, business areas, and model types/categories
- Risk Tier – A categorization of models, ranging from 1 to 3, that is used to differentiate validation and annual review requirements for models based on model risk
- Provisional Approval – An exception allowing the use of a business-critical model that does not have sufficient time to undergo the complete validation process
- Procedures – Documents that detail specific processes in line with Standards. Procedures may be enterprise-wide, for specific OEs, or for specific business areas
- Standards – Documents establishing requirements and controls to ensure that the Policy is carried out and interpreted consistently across SHUSA
- Temporary Exception – An exception allowing the use of a business-critical model that fails validation
- Vendor Model – A model procured from a third party

8.3 Appendix C - Key Contacts

Title	Role	Name and contact
Chief Model Risk Officer	Author and Owner of Policy	Rafic Fahs
Head of Model Governance	Oversees MRM Governance	Peter Walsh

8.4 Appendix D - Regulatory Obligations Addressed by the Policy

Regulatory agency	Citation	Title
Federal Reserve/OCC	http://www.federalreserve.gov/bankinforeg/srletters/sr1107.htm	SR Letter 11-7 Supervisory Guidance on Model Risk Management
Federal Reserve	http://www.federalreserve.gov/bankinforeg/basel/files/bcc1303.pdf	BCC 13-3 Guidance for Independent Verification of a Banking Organization's Advanced Approaches Systems

8.5 Appendix E - Related Frameworks, Policies, and Process and Administrative Documents

Document type	Entity and department	Owner	Document title and location
Framework	Banco Stander, S.A. General Risk Directorate	General Risk Directorate	Santander Group Model Risk Framework
Framework	SHUSA Risk Management	CRO	SHUSA Enterprise Model Risk Management Framework
Process and Administrative Document	SHUSA MRMG	CMRO	SHUSA Model Identification Procedures
Process and Administrative Document	SHUSA MRMG	CMRO	SHUSA Expert Judgment Model Standards
Process and Administrative Document	SHUSA MRMG	CMRO	SHUSA Model Validation and Annual Review Procedures

Document type	Entity and department	Owner	Document title and location
Process and Administrative Document	SHUSA MRMG	CMRO	SHUSA Model Development Standards
Process and Administrative Document	SHUSA MRMG	CMRO	SHUSA Model Validation Standards
Process and Administrative Document	SHUSA MRMG	CMRO	SHUSA Model Implementation Standards
Process and Administrative Document	SHUSA MRMG	CMRO	SHUSA Model Use Standards
Process and Administrative Document	SHUSA MRMG	CMRO	SHUSA Ongoing Model Management Standards
Process and Administrative Document	SHUSA MRMG	CMRO	SHUSA MRM Compliance Standards