**Santander Holdings USA**



**Enterprise Risk Management Framework**

**Table of Contents**

[1. Introduction - 4 -](#_Toc437479759)

[1.1 Background - 4 -](#_Toc437479760)

[1.2 Scope - 4 -](#_Toc437479761)

[1.3 Purpose of the Enterprise Risk Management Framework - 4 -](#_Toc437479762)

[1.4 Document Ownership and Maintenance - 5 -](#_Toc437479763)

[2. Definition of Enterprise Risks – The SHUSA Risk Taxonomy - 6 -](#_Toc437479764)

[3. Enterprise Risk Management Principles - 7 -](#_Toc437479765)

[3.1 Risk Culture - 7 -](#_Toc437479766)

[3.2 Risk Management Accountability Principles - 7 -](#_Toc437479767)

[3.3 Risk Management Governance - 8 -](#_Toc437479768)

[3.4 Risk Appetite Statement - 8 -](#_Toc437479769)

[3.5 Enterprise Risk Management Frameworks, Policies and Procedures - 9 -](#_Toc437479770)

[3.6 Risk and compensation - 9 -](#_Toc437479771)

[4. SHUSA ERM Roles and Responsibilities - 10 -](#_Toc437479772)

[4.1 SHUSA ownership structure - 10 -](#_Toc437479773)

[4.2 SHUSA senior management committees - 10 -](#_Toc437479774)

[4.3 The SHUSA Board of Directors - 11 -](#_Toc437479775)

[4.4 The Chief Executive Officer - 11 -](#_Toc437479776)

[4.5 The Chief Risk Officer - 11 -](#_Toc437479777)

[4.6 Key Risk Management Committees - 13 -](#_Toc437479778)

[4.6.1 The Board Risk Committee - 13 -](#_Toc437479779)

[4.6.2 The Executive Risk Management Committee (“ERMC”) - 13 -](#_Toc437479780)

[4.6.3 The Operational Risk Management Committee (“ORMC”) - 13 -](#_Toc437479781)

[4.6.4 Model Risk Management Committee (“MRMC”) - 13 -](#_Toc437479782)

[4.6.5 Compliance Committee - 14 -](#_Toc437479783)

[4.6.6 Allowance for Loan and Lease Losses (“ALLL”) Committee - 14 -](#_Toc437479784)

[4.6.7 Market Risk Committee - 14 -](#_Toc437479785)

[4.7 Three Lines of Defense (“LoD”) - 14 -](#_Toc437479786)

[5. SHUSA Risk Organization - 19 -](#_Toc437479787)

[5.1 Overview - 19 -](#_Toc437479788)

[5.2 Risk Management Function - 19 -](#_Toc437479789)

[5.3 The ERM Risk Managers - 19 -](#_Toc437479790)

[5.4 The Enterprise Risk Management unit - 19 -](#_Toc437479791)

[5.5 SHUSA and Operating Entity Risk Management Organizations - 20 -](#_Toc437479792)

[6. ERM Frameworks, Policies and Procedures - 21 -](#_Toc437479793)

[7. ERM Methodology - 22 -](#_Toc437479794)

[7.1 Risk Identification, Assessment, Control, Residual Risk and Reporting - 22 -](#_Toc437479795)

[7.2 The ERM Methodology cycle - 22 -](#_Toc437479796)

[8. Document History and Version Control - 25 -](#_Toc437479797)

[8.1 Ownership and Authorship - 25 -](#_Toc437479798)

[8.2 Sign-Off - 25 -](#_Toc437479799)

1. Introduction
   1. Background

The identification, assessment, control, monitoring, testing and reporting of risks across all risk types, together with the clear articulation and communication of risk appetite, provide the foundation for the SHUSA risk management program. This program is based upon successful implementation of a forward looking risk management culture to strengthen SHUSA’s resilience to shocks, whether originating internally or externally, thereby promoting a stable environment for business activities. Success in managing risk as outlined in this Framework is demonstrated by SHUSA establishing and maintaining an organizational culture that embraces by its actions prudent risk taking and integrates risk management processes within its day-to-day operations.

* 1. Scope

The Santander Holdings USA, Inc. (“SHUSA” or “the Company”) Enterprise Risk Management (“ERM”) Framework applies to SHUSA and its Operating Entities[[1]](#footnote-2) (together “the Enterprise”), which are separately chartered U.S. domiciled financial services companies.

This ERM Framework describes the high level principles for the management, control and oversight of risk across all business activities and support functions of the Enterprise. These principles must also be applied to the management of all third parties that provide services to SHUSA, its Operating Entities and its customers.

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

* 1. Purpose of the Enterprise Risk Management Framework

This ERM Framework describes the program through which SHUSA will oversee the risks arising from its business activities and operations and govern its risk management activities.

The goal of ERM is to manage risks across the consolidated organization in a comprehensive, consistent and effective fashion, enabling the firm to achieve its strategic priorities, including its business plan, within its expressed risk appetite. SHUSA’s ERM program is designed to achieve effective risk management in a consistent fashion across the Enterprise and is in compliance with all applicable rules, regulations and guidance. Moreover, it is designed to provide early recognition and effective management of risks emerging from changes in SHUSA´s risk profile or from external or systemic sources and to be refined as the risks and risk profile of SHUSA changes. Thus, the Framework contemplates controlling and monitoring known risks and the timely identification and effective management of new and changing risks.

This Framework is aligned to the General Risk Framework approved by the Board of Directors of Banco Santander S.A. (“Santander” or the “Group”), and adopted by the SHUSA Board, that establishes the principles that must be followed by all Santander Group entities when managing and controlling all risks.

* 1. Document Ownership and Maintenance

As owner, the SHUSA Chief Risk Officer (CRO) is responsible for the maintenance of this Framework. It is approved by the SHUSA Board of Directors (“Board”) under recommendation from the SHUSA Executive Risk Management Committee (“ERMC”) and the SHUSA Board Risk Committee (“RC”)[[2]](#footnote-3).

The Framework must be reviewed at least annually and updated as necessary in the event of material changes to the risk profile of SHUSA, be it directly or through a change in the risk profile of its Operating Entities, including regulatory changes. Material changes, relating to the way risks need to be managed and controlled, will be approved by the Board. 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, RC and Board.

1. Definition of Enterprise Risks – The SHUSA Risk Taxonomy

The following are the defined key risk types that need to be considered and managed in each business decision and in the day to day operations of SHUSA and its Operating Entities. Specific frameworks or policies are in place for certain risk types, and they detail how they are identified, measured, controlled, monitored and reported.

| **Risk Type**  **Risk Sub-Category** | **Definition** |
| --- | --- |
| **Capital Adequacy1** | Capital Adequacy risk is the risk that the company may not hold sufficient capital to ensure its safety and soundness, to support its business plans, to satisfy current and future regulatory and internal capital requirements and to meet market expectations. |
| **Credit2** | Credit risk is the risk to current or anticipated earnings or capital arising from an obligor's failure to meet the terms of any contract with the bank or otherwise perform as agreed. |
| **Residual Value3** | Residual Value (RV) risk is the risk of financial loss that may occur if, at the end of a lease contract, even if the obligor has complied fully with his financial obligations under the contract, the actual proceeds realized upon the sale of returned assets are lower than the projection of the expected value used in establishing the pricing at lease origination. |
| **Liquidity2** | Liquidity risk is the risk that the company would be unable to meet its obligations when they come due without incurring unacceptable losses. The firm, although solvent, either does not have available sufficient financial resources to enable it to meet its obligations as they fall due, or can secure them only at excessive cost. |
| **Market (Trading and Banking Book)2** | Market risk is the risk to current or anticipated earnings or capital resulting from adverse movements in market rates or prices, including, but not limited to, interest rates, foreign exchange rates, or equity prices. |
| **Operational** | Operational risk is the risk of loss resulting from inadequate or failed processes, people, systems, or from external events. This definition includes legal risk and fraud risk but excludes strategic and reputational risk. |
| **Model2** | Model risk is 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 the firm’s reputation. |
| **Strategic** | Strategic risk is the risk of not achieving the strategic business plan due to adverse business decisions, lack of responsiveness to industry or environmental changes or poor implementation of decisions through inappropriate deployment of resources. |
| **Reputational** | Reputational risk is the risk of damage to the way the company is perceived by public opinion, by its clients, investors, regulators or any other interested party. |
| **Compliance1** | Compliance risk is the risk arising from violations of laws, rules, or regulations, or from non-conformance with prescribed practices, internal policies and procedures, or ethical standards. |
| **Financial Crime4** | Financial Crime risk is the risk that the company is used for activities such as money laundering, terrorist financing, sanctions and bribery & corruption. |
| **Conduct Risk4** | Conduct risk is the risk that the company’s decisions and behaviors lead to a detriment or poor outcomes for its customers and that the company fails to hold to and maintain high standards of market integrity. |

1Specific Policy. 2Specific Framework. 3Included in Credit Risk Framework. 4Included in Compliance Framework

1. Enterprise Risk Management Principles
   1. Risk Culture

A strong risk management culture supports SHUSA´s long term success. This culture is evidenced by actions in which financial objectives are determined and are achieved by means of careful selection and management of risks and where risk identification, management and control are integrated into all business decisions.

Through its Code of Conduct the Board of SHUSA has communicated the values and behaviors it expects the staff of SHUSA and its Operating Entities to adopt in their daily activities. In addition to these values and behaviors, the ERM Framework describes the principles through which the Board of SHUSA seeks to establish a risk culture that embeds risk management into its daily processes and procedures, and synchronizes core risk management activities across the Enterprise. This requires that the nature and size of risks are well understood and communicated, risk-taking is transparent, decision-making is effective and decision-makers accountable, and that risks are identified, measured, controlled, monitored and reported appropriately.

Establishing a culture in which these practices are embedded across SHUSA and all of its Operating Entities needs to include the identification of risks that may not be readily captured by formal processes and the communication of those risks so they are appropriately addressed. These practices are essential to the integration of risk management and compliance controls with management goals and the Enterprise compensation structure.

* 1. Risk Management Accountability Principles

The following are the SHUSA risk management accountability principles, applicable throughout the organization:

* **Transparent accountability** – Accountability for risk management activities and decision making are defined in this Framework through the Roles and Responsibilities for ERM management. The level of accountability will be reflected in all risk type frameworks and in the relevant ERM Policies and Operating Entity policies.
* **Performance and compensation** – in combination with Human Resources policies and procedures, risk appetite and underlying business line metrics along with any other appropriate criteria that is identified will be incorporated into objectives that will be included in individual performance plans, aligning compensation to risk management goals.
* **Ongoing support** – It is the responsibility of the SHUSA Board and the Operating Entity Boards to ensure that sufficient and competent risk management resources are deployed throughout the organization, and that risk training is provided to all staff as required.
  1. Risk Management Governance

The following are the management governance principles that are applicable to SHUSA and its Operating Entities:

* **Defined authority** – The SHUSA Board will ensure, through the implementation of its Governance Framework[[3]](#footnote-4), that the SHUSA management teams establish separate and focused governance processes including committees and delegated authorities to oversee the operations of their respective functions at the level of SHUSA and its Operating Entities.
* **Clear oversight and issue escalation processes** – Risk governance structures established by the Board at SHUSA will ensure that responsibility for oversight and reporting and the processes for escalating issues are understood and followed throughout the organization.
* **Independent structure** – The SHUSA Board will ensure the development and maintenance of independent risk management functions and risk governance structures that are communicated and understood throughout the organization.
* **Effective Challenge** – Effective management challenge processes are required to be established as part of the risk governance structures to ensure adequate oversight of risk-taking and risk management activities. Effective challenge includes dedicated oversight and review by an independent risk management function, the Board where applicable, and an internal audit function vested with appropriate stature and authority.
  1. Risk Appetite Statement

The SHUSA Enterprise Risk Appetite Statement (“RAS”) is approved by the SHUSA Board. It defines the aggregate levels and types of risk that SHUSA and its Operating Entities are willing to accept in the pursuit of their strategic objectives. It is the overarching mandate governing all risk-taking activities across the organization and it is arrived at through a process that identifies risks and quantifies the amount of risk and the circumstances under which SHUSA is willing to accept those risks.

The SHUSA Enterprise RAS is proposed by the CEO to the SHUSA Board. It must be updated on an annual basis, or as-needed in response to significant change in the Company or the Enterprise’s risk profile. All updates are to be reviewed and challenged through the appropriate committee process at both the SHUSA and Operating Entity level and the CRO will provide advice to the SHUSA ERMC, the SHUSA RC, and the SHUSA Board on the RAS associated with the business plan and on its appropriateness.

SHUSA Operating Entities are responsible for developing and approving their own risk appetite statements with proper review and challenge according to their respective governance structures, and in consultation with the SHUSA CEO and CRO. The Operating Entities´ CROs are accountable for ensuring that their risk appetite statements are aligned to the SHUSA RAS limits. The Operating Entity-level RAS will be cascaded down through more detailed limits appropriate to each line of business within the Operating Entities.

The SHUSA CRO is responsible for overseeing the monitoring of compliance with the SHUSA RAS limits, ensuring consistency between appetite, capital, limits and the strategic business plans. Operating Entities’ CROs are responsible for overseeing the monitoring of compliance with their respective RAS limits. Risk taking in excess of appetites shall be escalated with accompanying remediation plans and monitored through the risk management committee governance process.

* 1. Enterprise Risk Management Frameworks, Policies and Procedures

A comprehensive inventory of Frameworks, Policies, and and Procedures must be established and maintained by SHUSA and its Operating Entities covering all risk types, to ensure that risk management and controls are executed in accordance with the ERM requirements prescribed in this Framework.

SHUSA´S CRO and Risk Management team will evaluate the comprehensiveness and alignment of the Operating Entities’ policies, monitor their compliance, and report on their status to senior management and the Board.

All employees are to be made aware of the documents relevant to them in their day to day activities.

* 1. Risk and compensation

The objective setting, performance management and compensation programs must be aligned to risk management objectives. To be considered properly functioning programs they must avoid incentivizing inappropriate risk taking activities.

Performance against risk objectives must be appraised, documented and linked, where appropriate, to quantitative measures.

1. SHUSA ERM Roles and Responsibilities
   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 on its risks and risk management activities to the Santander S.A. Global Risk function on a periodic basis.

* 1. SHUSA senior management committees[[4]](#footnote-5)

SHUSA implements its governance process through a hierarchy of board- and management-level committees with defined decision-making authorities detailed in their charters. These committees are responsible, along with management, for establishing and implementing risk type frameworks and ERM policies that give effect to this ERM Framework. The SHUSA committee structure is outlined below, and it expects its Operating Entities to adopt and adapt this structure when establishing their independent governance and decision-making bodies and defining their charters.



**CEO = Chief Executive Officer; CFO = Chief Financial Officer; CRO = Chief Risk Officer; CIA = Chief Internal Auditor; CLO = Chief Legal Officer;**

**CCO = Chief Compliance Officer; Head of Financial Control**

* 1. The SHUSA Board of Directors

The SHUSA Board is responsible for SHUSA’s oversight.

With respect to governance, implementation, and monitoring of the Risk Framework, the SHUSA Board is responsible for reviewing and approving the Framework and certain key Risk Policies, overseeing implementation of the Framework, and monitoring compliance with the Policies.

These responsibilities will also be reflected in the charters of the Boards of the SHUSA Operating Entities.

* 1. The Chief Executive Officer

The Board delegates full oversight responsibility to the SHUSA Chief Executive Officer (CEO) for the execution by management of risk monitoring and control related activities on a day-to-day basis.

The main risk management responsibilities of the CEO are:

* Propose the Risk Appetite Statement;
* Ensure the establishment, implementation and maintenance of appropriate risk processes that meet regulatory expectations and support, from a risk perspective, the effective delivery of the strategic objectives and business plan;
* Report on a regular basis to the Board on the management and control of the key risks to achieving the SHUSA business plan; and
* Ensure that a corporate culture promoting a strong risk culture backed by ethical practices is fostered in SHUSA and that the corporate values approved by the Board are effectively communicated and implemented throughout the organization so that its business plan and strategic objectives are aligned with its culture, values and ethics
  1. The Chief Risk Officer

As an independent executive that leads the SHUSA Risk organization[[5]](#footnote-6), the SHUSA CRO reports to the SHUSA RC and the SHUSA CEO. The SHUSA RC reviews the CRO’s performance and has the authority to approve his/her retention and dismissal.

The main responsibilities of the CRO are:

* The design, recommendation, implementation, oversight, and administration of the SHUSA ERM Program in line with all regulatory requirements and risk profile changes;
* The oversight, review, challenge, recommendation of changes, and control of the SHUSA Risk Appetite process;
* The implementation of risk appetite limits for SHUSA, and oversight of the implementation of risk appetite limits by its Operating Entities consistent with SHUSA risk appetite limits;
* Monitoring and reporting on compliance with risk appetite limits;
* The coordination and synchronization of key activities across all Operating Entities in order to effectively integrate risk management processes with the risk aspects of other processes such as capital planning, liquidity planning, strategic planning, stress testing, compensation and regulatory submissions;
* Overseeing projects designed to enhance the enterprise risk management process;
* Overseeing the creation and implementation of, and compliance with, ERM frameworks, policies and procedures;
* Overseeing the management of risks and risk controls within the parameters of the ERM Program and monitoring of those risks and testing controls;
* Reporting risk management deficiencies, breaches of risk limits, and emerging risks through the committee process including directly to the ERMC, the RC and the Board; ensuring effective and timely implementation of related actions and monitoring those actions; and
* Representing risk management and the second line of defense in support of risk-related processes, including new products/business activities reviews and approvals, compensation planning, business strategy development, resolution matters, capital and liquidity stress-testing and contingency planning.
  1. Key Risk Management Committees

The risk management responsibilities, membership, and decision rights of key risk management committees are summarized below. In some cases, committees may recommend decisions for approval to a higher level committee or to the Board. Decisions that each committee must escalate for Board approval are outlined below. Further duties and details of responsibilities of committees, including the definition of which decisions are considered material, may be found in their respective charters.

* + 1. The Board Risk Committee

Assists the Board in its oversight responsibilities with respect to enterprise risk management activities and compliance matters across the Enterprise.

The RC is chaired by an independent Director and its membership consists of no fewer than three and no more than seven Directors, the majority of whom are non-executive members. The key point of contact within management for the Board Risk Committee is the CRO.

The RC approves the appointment, removal, and annual performance of the CRO. The RC oversees implementation of the ERM Framework.

The RC approves key risk-related documents (e.g. ERM frameworks and capital plans) and select policies (where regulation requires Board approval or where deemed appropriate by management), material remediation actions, and allowance for loan and lease losses (“ALLL”) levels.

* + 1. The Executive Risk Management Committee (“ERMC”)

Supervises the management of all risk types across SHUSA and its Operating Businesses. The Committee supports the RC in performing its responsibilities by supervising risk, escalating material issues to the Board, recommending certain key documents to the Board, and approving key policies and standards. The ERMC is co-chaired by the CRO and CEO, its membership includes Risk, Finance, and Business subject matter experts, and it reports to the RC.

* + 1. The Operational Risk Management Committee (“ORMC”)

Supports the ERMC on matters related to operational risk. The Committee approves certain operational risk policies and standards; monitors relevant metrics, provides input on assumptions and scenarios; and oversees business capabilities for managing operational risk. The Operational Risk Management Committee is chaired by the Chief Operational Risk Officer, its membership includes Risk, Finance, Legal, and Business line/ Technology & Operations experts, and it reports to ERMC.

* + 1. Model Risk Management Committee (“MRMC”)

Oversees model risk across the Enterprise and assists the RC and ERMC in managing model risk. The Committee’s primary role is the coordination and oversight of model risk. The MRMC is chaired by the Chief Model Risk Officer, its membership includes Risk, Finance, and Operating Business experts, and it reports to the ERMC.

* + 1. Compliance Committee

Supports the ERMC on matters related to compliance. The Committee ensures the observance of applicable laws, rules, and regulations. The Committee approves most compliance and ethics policies, and identifies, monitors, and escalates compliance risks, regulatory changes, and trends. The Compliance Committee is chaired by the Chief Compliance Officer, its membership includes Compliance, Legal, and Operating Business experts, and it reports to the ERMC.

* + 1. Allowance for Loan and Lease Losses (“ALLL”) Committee

Supervises the establishment of the Company’s loan and lease loss reserve level. The Committee supports the ERMC by supervising the ALLL process, escalating material issues to the ERMC, recommending policies to the ERMC, recommending to the Disclosure Committee a comprehensive report of the ALLL process, and approving ALLL standards and procedures. The ALLL Committee is chaired by the CRO, its membership includes Risk and Finance experts, and it reports to the ERMC and Disclosure committees.

* + 1. Market Risk Committee

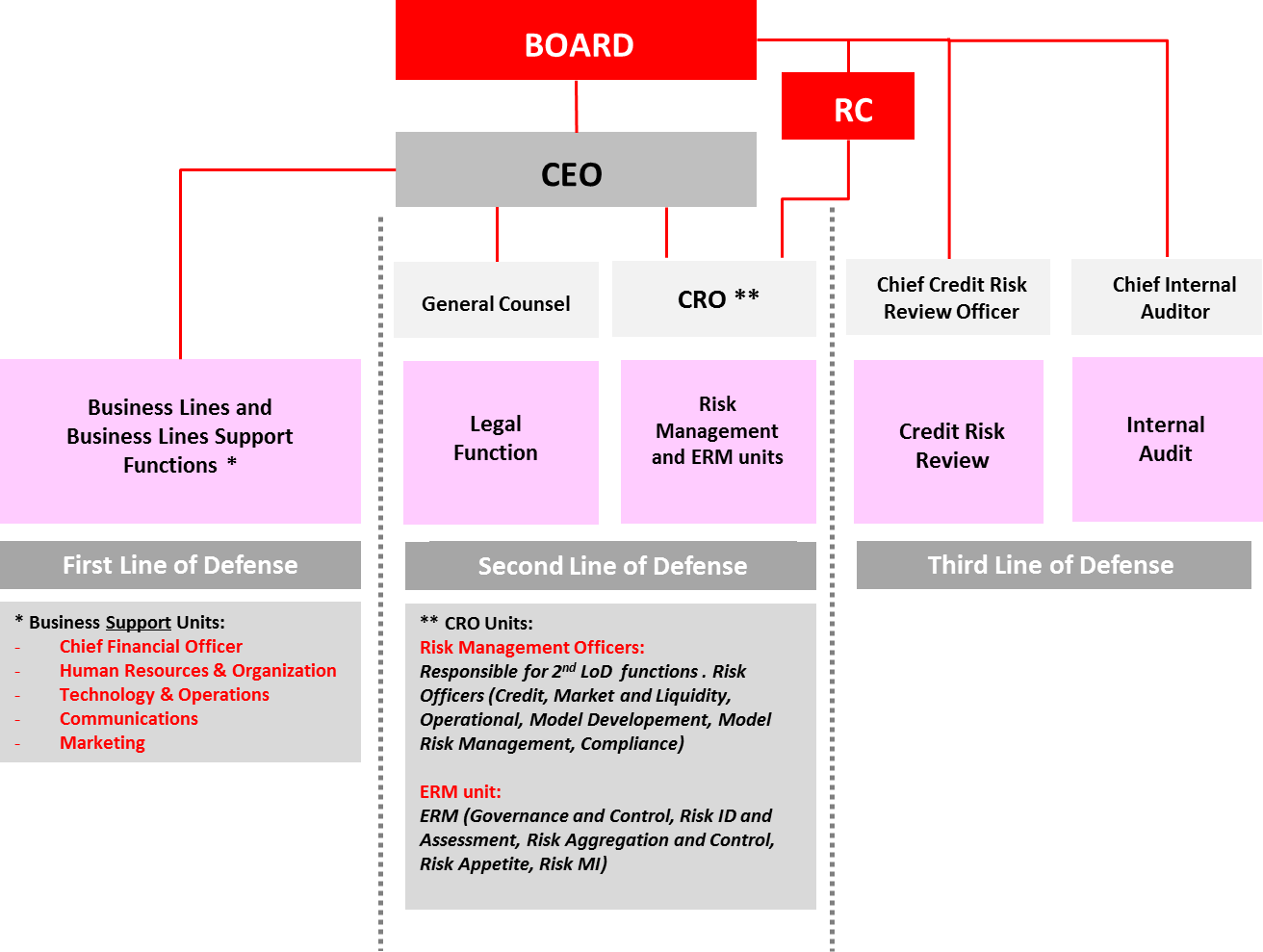
Supports the ERMC on matters related to liquidity risk and market risk, including interest rate risk and trading risk. The Committee approves market risk policies and standards; monitors market risk limits; and provides input on market and liquidity risk assumptions and scenarios. The Market Risk Committee is chaired by the Chief Market Risk Officer, its membership includes Risk, Finance, and Operating Business experts, and it reports to ERMC.

* 1. Three Lines of Defense (“LoD”)

SHUSA and its Operating Entities will organize their roles and responsibilities for risk management into a “three lines of defense” model, with separately defined and segregated responsibilities consistent with applicable regulations and guidance:

* **1st LoD – SHUSA, its Operating Entities and their Business Lines and Business Lines Support Units:** reporting to the CEO,1st LoD units have responsibility for the primary management of the risks that emanate from their activities. 1st LoD units own, identify, measure, control, monitor and report all risks that are originated through activities such as business origination, the development, marketing or distribution of products, client maintenance, or operational or technological processes supporting customer activity.
* **2nd LoD - ERM function and Risk Management functions** that are under the executive responsibility of the CEO but report to the CRO. These 2nd LoD units manage and monitor risk exposures, define frameworks, policies and comprehensive and appropriate controls, and ensure 1st LoD units manage risk in line with the agreed frameworks and risk appetite levels.
* **2nd LoD – Legal Function** that is under the executive responsibility of the CEO.
* **3rd LoD – Risk Assurance - Internal Audit; Credit Risk Review Function.** 
  + - ***Internal Audit*** provides independent assurance and reports to the Board. It is a permanent corporate function, independent of any other function or unit in SHUSA or its Operating Entities, whose purpose is to provide assurance to the SHUSA Board and Senior Management, thus contributing to the protection of the organization and its reputation, by assessing the quality and effectiveness of the processes and systems of internal control, risk management and risk governance; compliance with applicable regulations; the reliability and integrity of financial and operational information including the integrity of the balance sheet of SHUSA.
    - ***The Credit Risk Review Function*** reporting to the Board and administratively to the SHUSA CRO provides an independent assessment of SHUSA’s credit risk and credit risk practices to the Board. The primary goal of Credit Risk Review is to ensure credit practices are consistent with SHUSA’s desired risk profile and risk appetite limits.

A simplified Three LoD model is depicted below.



The responsibilities for each LoD are organized into three sub-categories: **Risk Identification and Assessment, Internal Controls and Monitoring, Testing, and Reporting.** The tables below define general three lines of defense risk management responsibilities across all risk areas, and the ERM Policies further specify particular three lines of defense roles and responsibilities as they pertain to individual risk areas.

|  |  |  |
| --- | --- | --- |
| **Risk Identification and Assessment** | | |
| **1st LoD** | * Develop the Strategic Planning process and Financial Planning according to predefined Top Down Risk Appetite * Participate in the Material Risk Program (e.g., in workshops as Business managers, subject matter experts) along with the 2nd LoD * Perform Risk Assessment including evaluation of inherent risk, quality of risk management controls and residual risks * Define Risk Materiality for the respective business area * Prepare Remediation Plans and develop corrective actions * Provide support to additional tasks related to the Capital Planning Process: a) Provide input to stress test scenario analysis; b) Identify sources of uncertainty for capital buffer estimation | |
| **2nd LoD** | **Risk Managers** | |
| * Support 1st LoD implementation of the risk framework, policies and procedures * Specify consistent risk identification and measurement processes across Operating Entities * Develop and own risk analyses and risk metrics for respective risk areas * Complete risk assessments * Conduct new product and new business activities risk  assessments * Provide risk input to business lines across the organization * Participate in the compensation, capital (CCAR), liquidity/funding (CLR) and strategic planning processes (risk input) * Manage loss forecasting processes and measurements and stress testing calculations | |
| **ERM unit** | |
| * Coordinate and ensure the consistency of the enterprise wide risk assessment framework across Risk Types and Operating Entities * Define and implement the ERM Methodology policies for risk identification across SHUSA and its Operating Entities * Facilitate and Aggregate the enterprise-wide risk management information and provide analysis on risks and emerging risks (e.g., dependencies, concentrations, correlations, etc.) * Coordinate the consolidated risk management input into the strategic, capital, and liquidity/funding planning processes * Coordinate and consolidate the scenario proposal and analyses of stress testing results | |
| **3rd LoD** | **Internal Audit** | * Evaluate that a well-developed risk-assessment methodology (e.g., policies and procedures) has been developed and drives the risk-assessment process * Analyze the effectiveness of all critical risk management functions, including governance, operations, and information systems * Evaluate risk management governance within the institution, including at the senior management level, and within all significant business lines |
| **Credit Risk Review** |

|  |  |  |
| --- | --- | --- |
| **Internal Controls** | | |
| **1st LoD** | * Develop and embed an appropriate risk culture across the enterprise * Ensure sufficiency of resources (HR and Systems) to manage and control risk * Ensure risks are considered in the development and maintenance of Policies, Procedures, and Processes * Adhere to the Risk Appetite Statement and ensure adequate  governance and controls * Ensure reporting plan in place (Indicators, KRIs, KPIs, Limits…) * Identify training needs, communicate to 2nd LoD and support rollout of training programs | |
| **2nd LoD** | **Risk Managers** | |
| * Establish and maintain ERM policies aligned with the risk framework and risk appetite * Review and opine on risk-relevant Policies and procedures set by the 1st LoD * Support 1st LoD in the development and allocation of risk appetite limits for the respective risk areas and provide input on underlying risk metrics * Reinforce a culture of risk awareness * Develop risk training * Conduct independent verification of compliance with the risk framework, policies and procedures * Provide risk performance input for compensation programs * Develop and own the risk Models * Validate all Models across the Enterprise | |
| **ERM unit** | |
| * Contribute to promote a consistent and risk sensitive culture across the enterprise * Coordinate the alignment of risk training across the enterprise * Coordinate the enterprise risk management framework enforcement of risk controls * Coordinate and consolidate the development of SHUSA risk appetite * Provide input, review and agree on risk appetite limits and underlying metrics proposed by risk management | |
| **3rd LoD** | **Internal Audit** | * Providing assurance on the appropriateness of Frameworks, Policies, Procedures, and processes and the design and effectiveness of controls * Identify control issues as part of its risk assessment processes and determine the impact of such issues on the overall risk profile * Evaluate risk management governance within the institution, including at the senior management level, and within all significant business lines |
| **Credit Risk Review** |

|  |  |  |
| --- | --- | --- |
| **Monitoring, Testing and Reporting** | | |
| **1st LoD** | * Manage risk taking activity * Provide Quality Assurance for 1st LoD, including reconciliations of results, balance sheet and activities * Execute controls and monitoring protocols for 1st LoD * Working with the Model Development function, define risk model usage, embed risk model ownership policies and procedures in 1st LoD activities, define and implement 1st LoD model documentation and controls * Prepare RAS underlying metrics (e.g. risk mandates) in coordination with 2nd LoD and update results periodically * Analyze data to evaluate root causes, trends and internal controls and to support management decisions * Perform self-testing in compliance with policies and guidelines and define remediation actions for failed tests * Run realistic crisis management exercises on an ongoing basis, evaluate the effectiveness of Incident Response Plans * Report on key, evolving and emerging risks * Report on RAS underlying metrics (e.g. risk mandates) * Escalate identified deficiencies as well as audit findings, regulatory reviews, etc. and report on status of Remediation Plans | |
| **2nd LoD** | **Risk Managers** | |
| * Establish a risk reporting framework which enables effective monitoring and reporting on risks by the 1st LoD * Design KRIs, KPIs and risk MIS for respective risk areas * Monitor and report on external emerging risks and potential threats * Establish and administer a centralised model risk management function coordinating all model risk activities across SHUSA and its Operating Entities * Monitor and aggregate reporting on standards, limits and appetites for respective risk areas * Oversee issue and remediation tracking, monitoring and escalation across the enterprise * Analyze risk information for inclusion in business performance and capital utilization * Escalate material compliance and risk issues * Monitor regulatory guidance and best practices for necessary improvements | |
| **ERM unit** | |
| * Aggregate, harmonize and consolidate risk MIS and other risk reporting at the SHUSA level and provide guidance/guidelines for underlying Operating Entities * Consolidate and Report on compliance with the risk framework at the SHUSA level * Coordinate, aggregate and correlate emerging and key risks * Escalate key issues and exposures to appropriate risk committees * Analyze SHUSA consolidated risk information for inclusion in business performance and capital utilization * Ensure risk consolidated information is considered and actioned, where appropriate, for strategic decisions | |
| **3rd LoD** | **Internal Audit** | * Understand risks faced by the institution and confirm that the Board of Directors and senior management are actively involved in setting and monitoring adherence to the institution's enterprise-wide risk appetite * Evaluate the credit risk reporting framework’s appropriateness for the organization in view of integrity, reasonableness, and speed of escalation * Report identified deficiencies in the reporting of risks relating to policies, procedures, processes and controls to senior management through the Audit Committee or the Risk Committee as applicable; evaluate that management establishes effective remediation plans * Monitor corrective action and conduct follow-up reviews to ensure recommendations have been addressed * Evaluate and report on the credit quality of the lending portfolios, including internal ratings; and the adequacy of loan loss provisions, * Recommending remedial actions where required |
| **Credit Risk Review** |

1. SHUSA Risk Organization
   1. Overview

Reporting to the CRO, the SHUSA risk management organization function operates independently of the 1st LoD to ensure that risks are identified and measured objectively and without influence from business performance objectives.

* 1. Risk Management Function

Reporting to the CRO, the Risk Management function is composed of two distinct areas: Risk Managers responsible for overseeing the risk types and an ERM unit responsible for risk management activities linked to the ERM program.

In addition, the Credit Risk Review function that reports independently to the Board has an administrative reporting line to the SHUSA CRO.

* 1. The ERM Risk Managers

Responsible for Credit Risk, Market and Liquidity Risk, Operational Risk, Model Development, Compliance Risk and Model Risk Management across SHUSA, the Risk Managers develop the ERM Risk Type Frameworks and related ERM Policies for their risks, facilitating and overseeing Operating Entity implementation of the Operating Entity Frameworks and Policies, ensuring compliance with the related ERM policies, and proposing, assessing, controlling, reporting and monitoring risk appetite and limits for their respective risk areas.

Detailed roles and responsibilities for the Risk Managers with respect to Risk Identification and Assessment, Internal Control, and Monitoring, Testing and Reporting are set forth in the appropriate ERM Frameworks and Policies.

* 1. The Enterprise Risk Management unit

Covering the areas of Governance and Control Processes, Risk Management Information (“MI”), Material Risks Program, Risk Aggregation and Control and Risk Appetite, the ERM unit is responsible for the development and implementation of the ERM Framework, coordination of internal reporting to senior committees including the Board, project oversight for the ERM function, the ERM technology and data strategies, the production of MI including regulatory reporting, Risk ID and Material Risks Program, Risk Appetite Statement, Risk Aggregation, and the analysis and reporting of MI to the relevant committees and senior management.

* 1. SHUSA and Operating Entity Risk Management Organizations

Each SHUSA Operating Entity will maintain its own risk management organization structure that reflects the SHUSA structure as applied to the Operating Entity based on their business model, size and complexity. This will include both the risk management organization and the committee structures. Each Operating Entity risk organization will report hierarchically to its respective Board of Directors and CRO through this risk management organization and committee structure. The Operating Entity risk management organizations are directly accountable to the SHUSA risk organization for the implementation of the ERM Framework and for operating in accordance with it. This includes, where applicable, reporting from the Operating Entity CROs to the SHUSA CRO and from the Operating Entity risk officers to the respective SHUSA risk officers.

This structure is in place to maintain the integrity of SHUSA’s individual Operating Entities, and the accountability of their Boards of Directors and of executive management for their performance. Through the defined control and reporting responsibilities of Operating Entity CROs and their risk officers to the SHUSA risk function, SHUSA provides risk management oversight, ensures effective controls, and implements an integrated enterprise-wide risk framework through coordination with the risk officers within SHUSA and each Operating Entity.

1. ERM Frameworks, Policies and Procedures

SHUSA ERM Frameworks and Policies define the processes for identifying and reporting risks and risk management deficiencies, including emerging risks, on an enterprise-wide basis. Each policy establishes the requirements for the identification, assessment, control, monitoring, testing and reporting of the respective risk type, defining minimum standards and principles and taking into account best practices and regulatory requirements, ensuring a unified approach to the management of risks across SHUSA and its Operating Entities. Each of the Frameworks and Policies will set forth the respective roles and responsibilities for risk management by 1st LoD and 2nd LoD staff.

As new risks emerge and existing risk types change, new enterprise policies will be added or existing ones modified to reflect those changes. ERM Frameworks and Policies that are developed by SHUSA will apply to SHUSA and all Operating Entities. Operating Entities are expected to adhere to the principles embodied in the SHUSA ERM Frameworks and Policies through the development of Operating Entity Frameworks and Policies tailored to the specific needs of the Operating Entity and aligned with the requirements of the SHUSA ERM Frameworks and Policies.

The SHUSA policy hierarchy incudes ERM Policies, Policies and Process and Administrative documents. A full description of each type of document and their approval paths are included in the SHUSA Enterprise Policy Administration policy.

1. ERM Methodology
   1. Risk Identification, Assessment, Control, Residual Risk and Reporting

SHUSA manages its risks through the application and operationalization of the elements of risk management: **Risk Identification and Risk Assessment, Internal Controls, Monitoring, Testing, and Reporting:**

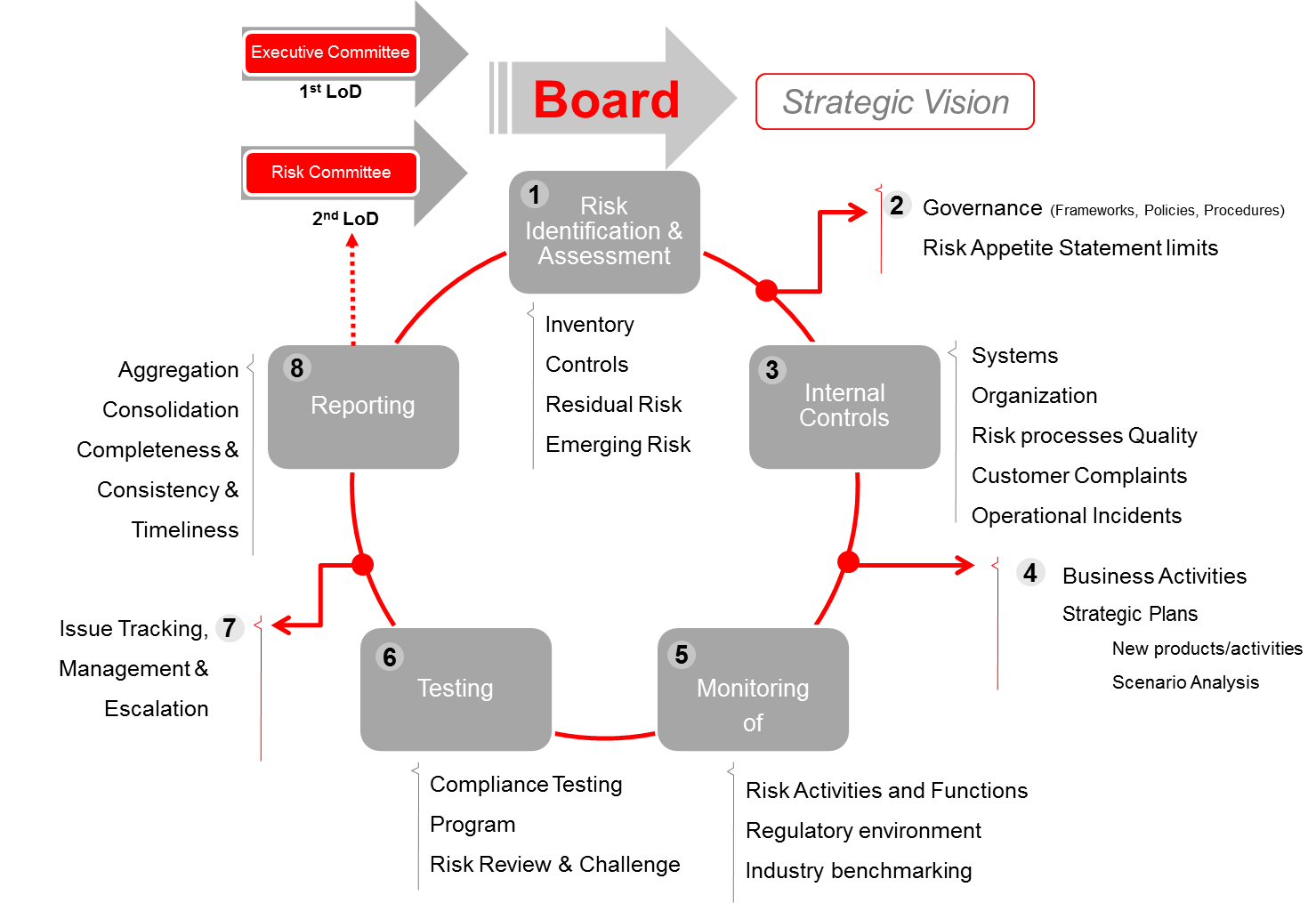
* **Risk identification** must be undertaken both at initiation of an activity and as an activity or the risks change with circumstances both internal and external to the organization.
* **Risk assessment** is the process by which all identified risks are measured for materiality. This process evaluates the size and/or materiality of each risk.
* **Definition and implementation of controls** that can be applied to each risk, where the design and implementation of these controls should be commensurate with the size of the risk being taken.
* **Residual risk** is the risk remaining in each business activity after considering the effectiveness of the internal controls. The residual risk is assessed by the risk owner to ensure that it corresponds with the overall strategy of SHUSA and is consistent with capital allocations.
* **Risk reporting** is the means by which the SHUSA Board, its management committees and all other governance structures are informed of the risks and risk issues identified in the activities of the SHUSA Operating Entities.

These integrated processes apply to all risks and risk-types, and together form the core elements of the ERM Methodology. Each Operating Entity is expected to adopt and execute upon this program consistent with the nature and complexity of its risks and activities.

* 1. The ERM Methodology cycle

The ERM Methodology is based upon building blocks that, taken as a whole, ensure that an integrated set of processes are defined and implemented throughout the risk cycle[[6]](#footnote-7). All Frameworks and Policies must ensure that the ERM methodology is embedded across all risks and all the Enterprise.

The hallmark of an ERM methodology, as illustrated in the diagram below, is to continuously verify that the business model is sustainable, the risk identification, assessment, management and reporting is effective and consistent across all risks and lines of business, with back testing of models and outcomes embedded as part of the business cycle.



|  |  |
| --- | --- |
| 1. **Risk ID and Assessment**  * Material Risks Program:   + Risk inventory   + Risk measurement   + Risk quantification   + Risk controls and mitigants * Risk response – accept/ mitigate/ transfer / reject. * Risk Correlation * Emerging Risks | 1. **Governance**  * Governance of Risks (Risk Frameworks) * Policies * Procedures * New Product Approval * Cost management and effectiveness of controls * Organization, Staffing and Training   **Model Risk and Model Usage,**  **Risk Analytics and Capital Calculation**   * Risk Model development and validation * Risk Model User/ Owner governance and back testing * Loss identification and forecasting * ICAAP / CCAR * Liquidity stress testing   **Risk Appetite and Mandates**   * Risk Appetite Limits & Metrics * Risk Scoring, Risk Approvals & Mandates |
| 1. **Internal Control**  * Quality assurance and Control   + Systems   + Organization * Risk processes quality * Customer complaints * Operational incidents | 1. **Business Activities**  * Business plans * Commercial strategy * New Products * Business plan scenario analysis |
| 1. **Monitoring**  * Regulatory, Policy and Business * Industry benchmarking * Risk Activities and functions * Risk Limits, KRIs, KPIs, Risk Appetite Statement | 1. **Testing**  * Compliance Testing Program * Risk Review & Challenge |
| 1. **Issue tracking and Escalation** | 1. **Reporting**  * Risk Monitoring / Loan Quality * Risk Reporting * Risk Aggregation / Consolidation * Completeness, consistency & timeliness * Regulatory Reporting |

1. Document History and Version Control
   1. Ownership and Authorship

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Owner** | **Change** |
| 1.0 | 5.22.14 | CRO | CRO | Initial SHUSA ERM Framework |
| 2.0 | 1.8.15 | CRO | CRO | Update to key risks, inclusion of CEO, change to CRO function description, expansion on ERM Methodology components |
| 3.0 | January 2016 | CRO | CRO | Update to key risks, update to Committee Structure |

* 1. Sign-Off

|  |  |  |
| --- | --- | --- |
| **Approving Body** | **Governance Committee Approval or Endorsement** | **Final Approval Date** |
| SHUSA Board of Directors | Board Enterprise Risk Committee | 5.22.14 |
| SHUSA Board of Directors | Board Enterprise Risk Committee | 1.30.15 |
| SHUSA Board of Directors | Board Risk Committee | January 2016 |

1. Santander Bank N.A., Santander Consumer USA Inc, Banco Santander Puerto Rico, Banco Santander International, Miami, Santander Investment Securities (NY), Santander Securities (PR), Santander Financial Services (PR), Santander Asset Management. [↑](#footnote-ref-2)
2. For additional information about these committees, refer to section 4.6 of this Framework. [↑](#footnote-ref-3)
3. The SHUSA Board Governance Framework articulates, principally but not limited to, the areas of management and oversight reserved to the Board of SHUSA and how it exercises control of its Operating Entities, the role of the SHUSA CEO and other senior management executives, including the CRO, and the approval paths for key business decisions across SHUSA and its Operating Entities. [↑](#footnote-ref-4)
4. Under review, subject to changes of the Governance Framework [↑](#footnote-ref-5)
5. Please refer to Section 5 of this Risk Framework for a description of the SHUSA Risk organization [↑](#footnote-ref-6)
6. ‘Cycle’ denotes a conceptual relationship and not a calendar-based sequence. Each element of the cycle may become a priority for attention at any time, depending on developments in the risk or control environments. [↑](#footnote-ref-7)