Santander Holdings USA

ENTERPRISE RISK MANAGEMENT FRAMEWORK

Table of Contents

1. Introduction

1.1 Background

The identification, assessment, control, monitoring, testing and reporting of risks across all risk types, together with the clear articulation and communication of risk tolerance, provide the foundation for the SHUSA risk management program. This program is based upon successful implementation of a forward looking risk management 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.

1.2 Scope

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

This ERM Framework describes the high level principles for the management, control and oversight of risk across all business activities and support functions of SHUSA and its subsidiaries as U.S. regulated institutions. These principles must also be applied to the Company's management of all third parties that provide services to SHUSA, its subsidiaries 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.

1.3 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 enterprise risk management 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 tolerance. SHUSA's ERM Program is designed to achieve effective risk management in a consistent fashion across the organization 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 the 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.

1.4 Document Ownership and Maintenance

As owner, the SHUSA Chief Risk Officer (CRO) is responsible for the development and maintenance of this Framework. It is approved by the SHUSA Board of Directors ("Board") under recommendation from the SHUSA Enterprise Risk Management Committee ("ERMC") and the SHUSA Board Enterprise Risk Committee ("BERC")[1].

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 subsidiaries, 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, BERC and Board.

[1] For additional information about these committees, refer to section 4.6 of this Framework

2. Definition of Enterprise Risks – The SHUSA Risk Map

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 subsidiaries. Specific frameworks for each risk type detail how they are identified, measured, controlled, monitored and reported, with the exception of Reputational risk as it typically arises as a result of the crystallization of other risks and Strategic risk that is managed and controlled through the strategic planning process.

Risk Type	Definition
Strategic	Strategic risk is the current and prospective impact on earnings or capital arising from adverse business decisions, or lack of responsiveness to industry or environmental changes. This risk is a function of the compatibility of an organization's strategic goals, the business strategies developed and the resources deployed to achieve those goals, internal factors that could inappropriately weaken risk management practices or controls, the quality of implementation of plans and business strategies and industry factors such as competition and customer preference.
Reputational	Reputational Risk is the potential that a corporate practice, or a new fact or rumor concerning products and services sold by the firm or practices at the firm harms the public's perception, including that of investors, customers, regulatory bodies and rating agencies, of the corporation.
Credit	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.
Market	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.
Liquidity	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.
Operational	Operational risk is the risk to current or anticipated earnings or capital arising from inadequate or failed internal processes or systems, including IT and data management systems and processes, human errors or misconduct, or adverse external events. Operational losses may result from internal fraud; external fraud, inadequate or inappropriate employment practices or workplace safety; failure to meet professional obligations involving clients, products, and business practices; damage to physical assets; business disruption and system failures; or failures in execution, delivery, and process management. Operational losses from such events may occur directly, or indirectly, for example through litigation arising from an adverse event.
Compliance	Compliance risk, that includes Conduct 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. Compliance risk exposes the company to potential fines, civil money penalties, payment of damages, and voiding of contracts. Compliance risk can result in diminished reputation, reduced franchise or enterprise value, limited business opportunities, and lessened expansion potential.
Model	Model risk is the potential for loss arising when a financial model used to measure a firm's risks or to value transactions does not perform the tasks or capture the risks as intended. Typically this is due to a conceptual flaw, an implementation error, poor quality or missing data, or due to the model being used inappropriately or in error.

3. ERM Principles

3.1 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 strategic decisions.

Through its Values Statement and Code of Conduct the Board of SHUSA has communicated the values and behaviors it expects the staff of SHUSA and its subsidiaries 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 subsidiaries' 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.

3.2 Risk Management Accountability

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 subsidiary operating policies.

- **Performance and compensation** – in combination with Human Resources policies and procedures, risk tolerance 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 subsidiary 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.

3.3 Risk Management Governance

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

- **Defined authority** – The SHUSA board will ensure, through the implementation of its Governance Framework, 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 subsidiaries.

- **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.

3.4 Risk Tolerance Statement

The SHUSA Enterprise Risk Tolerance Statement ("RTS") is approved by the SHUSA Board. It defines the aggregate levels and types of risk that SHUSA and its subsidiaries 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 RTS 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's risk profile. All updates are to be reviewed and challenged through the appropriate committee process at both the SHUSA and subsidiary level and the CRO will provide advice to the SHUSA ERMC, the SHUSA BERC, and the SHUSA Board on the RTS associated with the business plan and on its appropriateness.

SHUSA subsidiaries are responsible for developing and approving their own risk tolerance statements with proper review and challenge according to their respective governance structures, and in consultation with the SHUSA CEO and CRO. The subsidiaries´ CROs are accountable for ensuring that

their risk tolerance statements are aligned to the SHUSA RTS limits. The subsidiary-level RTS will be cascaded down through more detailed limits appropriate to each line of business within the subsidiaries.

The SHUSA CRO is responsible for overseeing the monitoring of compliance with the SHUSA RTS limits, ensuring consistency between tolerance, capital, limits and the strategic business plans. Subsidiaries' CROs are responsible for overseeing the monitoring of compliance with their respective RTS limits. Risk taking in excess of tolerances shall be escalated with accompanying remediation plans and monitored through the risk management committee governance process.

3.5 Enterprise Risk Management Frameworks, Policies and Procedures

A comprehensive inventory of Frameworks, Policies, and Operating Policies and Procedures must be established and maintained by SHUSA and its subsidiaries 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 subsidiaries' 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.

3.6 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.

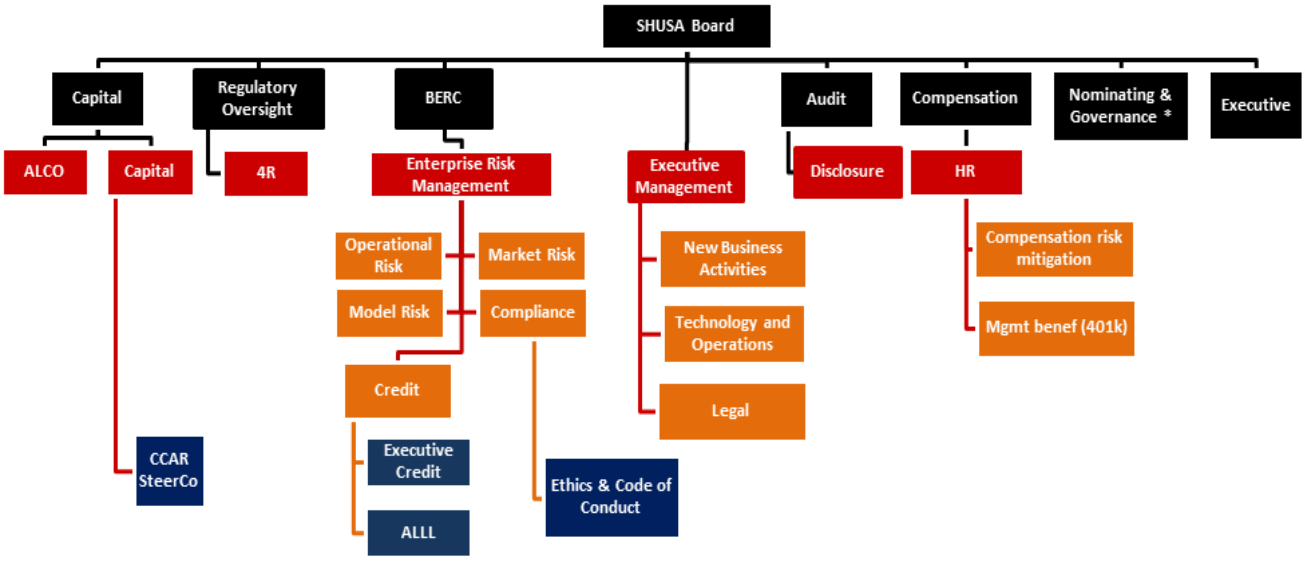
4. SHUSA ERM Roles and Responsibilities

4.1 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 Santander S.A.

4.2 SHUSA senior management committees

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 subsidiaries to adopt and adapt this structure when establishing their independent governance and decision-making bodies and defining their charters:



4.3 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 Enterprise 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 subsidiaries.

4.4 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 responsibilities of the CEO are:

- Propose the SHUSA business plan and strategy;
- Propose the Risk Tolerance 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

4.5 The Chief Risk Officer

As an independent executive that leads the SHUSA Risk organization[2], the SHUSA CRO reports to the SHUSA BERC and the SHUSA CEO. The SHUSA BERC reviews the CRO's performance and has the authority to approve his/her retention and dismissal.

The main responsibilities of the CRO are:

- The development, recommendation, 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 Tolerance process;
- The implementation of risk tolerance limits for SHUSA, and oversight of the implementation of risk tolerance limits by its subsidiaries consistent with SHUSA risk tolerance limits;
- Monitoring and reporting on compliance with risk tolerance limits;
- The coordination and synchronization of key activities across all subsidiaries 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 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 BERC 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.

[2] Please refer to Section 5 of this Risk Framework for a description of the SHUSA Risk organization

4.6 Key Risk Management Committees

4.6.1 The SHUSA Board Enterprise Risk Committee

The SHUSA BERC is established by and reports to the SHUSA Board to support the Board in its oversight responsibilities with respect to all risk-taking and risk management activities and compliance matters, including the following areas:

- Overseeing SHUSA's risk management organization, including reviewing the performance, and approving the retention or dismissal of the CRO;
- Reviewing and recommending to the Board for approval the consolidated Risk Assessment Summary which outlines the quantity of risk, quality of risk management, aggregate level of risk, and direction of risk of SHUSA and its subsidiaries;
- Reviewing and recommending for approval by the Board the ERM Framework and the Risk Tolerance Statement
- Approving risk type ERM Frameworks;
- Reviewing and approving the annual SHUSA Contingent Funding Plan;
- Overseeing an effective risk monitoring and reporting program;
- Reviewing and approving the annual work plan and resource budget for the CRO function;
- Overseeing the definition and successful execution of action plans to ensure enterprise wide compliance with the Risk Framework and the Risk Tolerance Statement; and
- Ensuring compliance with applicable regulations and guidance.

The SHUSA BERC will approve, receive reports on, and oversee the SHUSA risk management and regulatory compliance policies. The SHUSA BERC's charter will be approved by the board of directors and reflect a detailed description of the above listed responsibilities.

4.6.2 The SHUSA Enterprise Risk Management Committee

The ERMC is chaired by the SHUSA CRO. It is responsible for the oversight and monitoring of all risk-taking and risk management activities across the enterprise, including oversight of compliance matters.

The ERMC's core responsibilities include the following:

- Oversight of the development of the SHUSA ERM Framework and recommendation for its approval, subject to the concurrence of the Executive Management Committee, to the BERC and the Board and its implementation;
- Oversight of the development and recommendation of the Risk Tolerance Statement to BERC and its implementation;
- Oversight of the underlying risk committee structure and the administering of the ERM process throughout the organization;
- Oversight of monitoring and assessment of all SHUSA's risks through the underlying risk committee structure;
- Implementation of the ERM Program designed to evaluate and control risks throughout SHUSA;
- Oversight of the risk activities related to capital and liquidity stress testing and planning and analysis processes and ensuring their adequacy;
- Ensuring a risk monitoring and reporting program is in place that meets regulatory requirements;
- Oversight of escalation and reporting of key risks and issues to the BERC;
- Designate forums or subcommittees to support oversight and management of specific risks or risk areas;
- Reviewing regular reporting level of risks and exposures at SHUSA and its subsidiaries; and
- Providing strategic direction to the risk organization.

The SHUSA ERMC's charter will be approved by the board of directors and reflect a detailed description of the above listed responsibilities.

4.6.3 Level 2 Risk Management Committees and Sub-Committees

The charters of the committees include the detailed description of the responsibilities and relevant delegated authorities of each committee. A brief description is included below.

- ***Operational Risk:*** the SHUSA Operational Risk Committee is a management advisory, oversight and consultative committee, established under the specific authority of the SHUSA Enterprise Risk Management Committee and the SHUSA CRO to oversee operational risk in SHUSA´s operations and those of its subsidiaries.

- ***Market Risk:*** the SHUSA Market Risk Committee is a management committee, the purpose of which is to advise the SHUSA ERMC and the CRO with respect to the oversight of market risk management functions and the monitoring and evaluation of market, interest rate and liquidity risk in the SHUSA´s operations and those of its subsidiaries.

- ***Model Risk:*** the SHUSA Model Risk Management Committee is a management advisory, consultative, and approval committee established under the specific authority of the SHUSA Enterprise Risk Management Committee ("ERMC"). It is responsible for the supervision of model risk management across all SHUSA and its subsidiaries. The Committee is the final authority on what falls within the scope of SHUSA´s Model Risk Management Policy and is responsible for resolving model risk management issues on an escalated basis.

- ***Compliance:*** the SHUSA Compliance Committee oversees the compliance risks of SHUSA and its subsidiaries to ensure regulatory compliance with all applicable laws, rules and regulations (including banking and non-banking laws, rules, regulations and supervisory guidance), to verify compliance with established US enterprise compliance standards, to monitor the completion of annual compliance plans, and to identify and escalate material compliance issues. The committee has the delegated authority from ERMC to approve relevant compliance policies, risk assessments, and analysis reports.

- ***Credit Risk:*** the SHUSA Credit Risk Committee is a management advisory, oversight and consultative committee, established under the specific authority of the SHUSA Enterprise Risk Management Committee to oversee and manage the identification, monitoring and evaluation of credit risk in SHUSA´s operations and those of its subsidiaries, including methodologies, calculations and controls of key credit risk metrics.

    - ***Executive Credit Committee:*** is a management committee established under the Charter of the SHUSA Credit Risk Committee. It reviews, recommends and approves as set out in

its charter, individual lending transactions, limit pre-classifications, leveraged buy-outs, purchases and / or sales of portfolios and Strategic Commercial Plans[3] ("SCPs").

- ***Allowance for Loan and Lease Losses ("ALLL") Committee:*** is a management committee that oversees and ensures consistency and accuracy in the application of the methodology, calculation, monitoring, reporting and control of the loan and lease loss reserve processes at SHUSA and its subsidiaries.

4.7 Three Lines of Defense

SHUSA and its subsidiaries 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:

- **Line 1 Risk Management – SHUSA, its Subsidiaries and their Lines of Business & Lines of Business Support Units:** reporting to the CEO, Line 1 units have responsibility for the primary management of the risks that emanate from their activities. Line 1 units own, identify, measure, control, monitor and report all risks that are originated through activities such as business origination, providing specialist advice, the development, marketing or distribution of products, client maintenance, or operational or technological processes supporting customer activity.

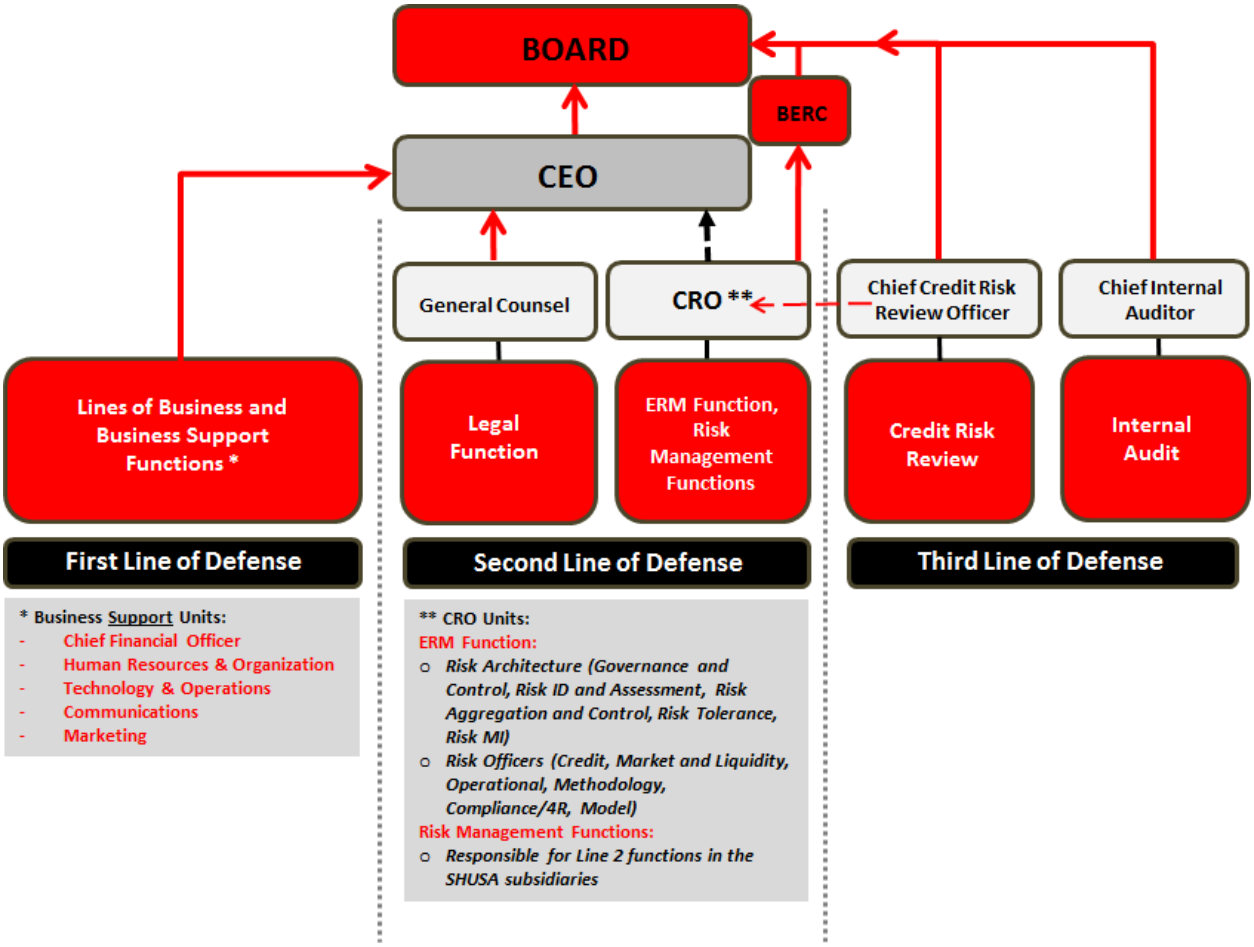
- **Line 2 ERM Function and Risk Management Functions** that are under the executive responsibility of the CEO but report to the CRO. These Line 2 units manage and monitor risk exposures, define frameworks, policies and comprehensive and appropriate controls, and ensure Line 1 units manage risk in line with the agreed frameworks and risk appetite levels.
- **Line 2 Legal Function** that is under the executive responsibility of the CEO.

- **Line 3 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 subsidiaries, 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.

[3] SCPs are frameworks produced jointly by the lines of business of SHUSA's subsidiaries and their Credit Risk teams and that define the risk appetite and credit limits for each line of business under agreed credit lending criteria.

- ***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 tolerance limits.

A simplified Three Lines of Defense model is depicted below.



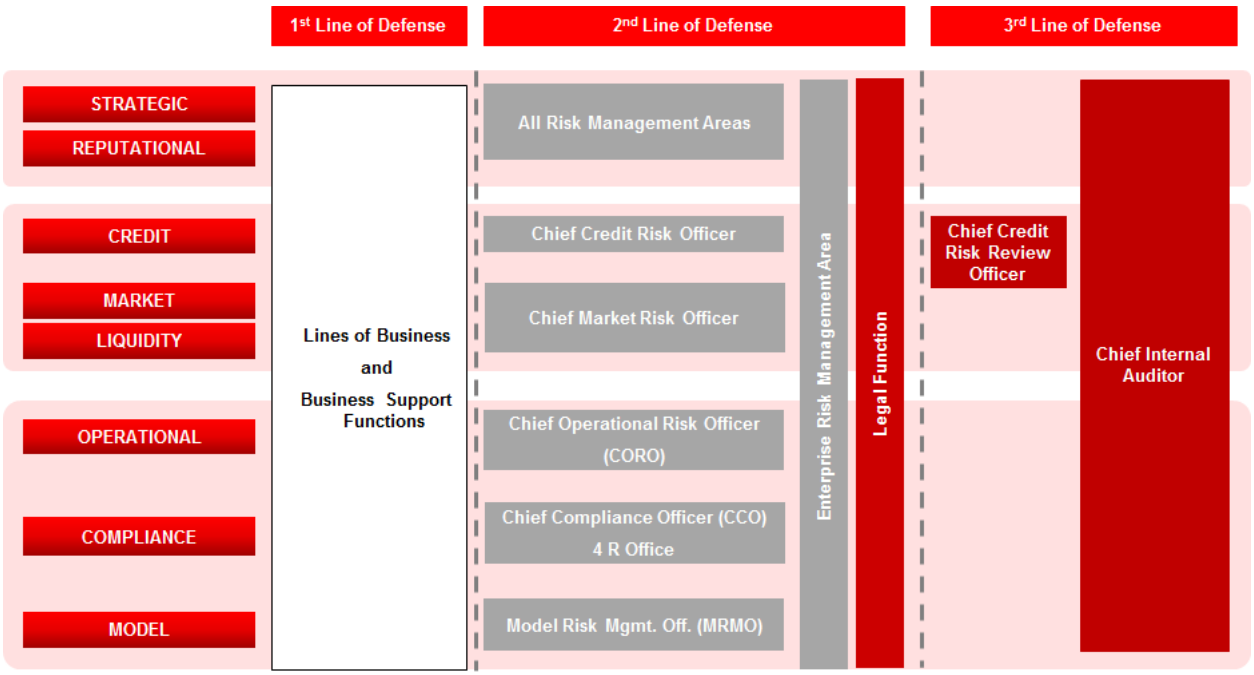
The responsibilities for each line of defense are organized into three sub-categories: **Identification and Assessment, Internal Controls and Monitoring, Testing, and Reporting.** The table below defines general three lines of defense risk management responsibilities across all risk areas, and the ERM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

Identification and Assessment			
Line 1	**Line 2**		**Line 3**
Business Acts. / Corp. Functions	***ERM Program***	***Risk Management Areas***	***Internal Audit/Credit Risk Review***
• Develop the Strategic Planning process and Financial Planning according to predefined Top Down Risk Tolerance • Participate in Risk Identification process (e.g., in workshops as Business managers, subject matter experts…) along Line 2 • Perform Risk Assessment including evaluation of inherent risk, quality of risk management controls and residual risks • Define Risk Materiality for respective risk 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	• Coordinate and ensure the consistency of the enterprise wide risk assessment framework across Risk Types and subsidiaries • Define and implement the ERM Methodology policies for risk identification across SHUSA and its subsidiaries • 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	• Support Line 1 implementation of the risk framework, policies and procedures • Specify consistent risk identification and measurement processes across subsidiaries • 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	• 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

Internal Controls			
Line 1	**Line 2**		**Line 3**
Business Acts. / Corp. Functions	***ERM Program***	***Risk Management Areas***	***Internal Audit/Credit Risk Review***
• 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 operating Policies, Procedures, and Processes • Adhere to the Risk Tolerance Statement and ensure adequate governance and controls • Ensure Reporting Plan in place (Indicators, KRIs, KPIs, Limits…) • Identify Training Needs, communicate to Line 2 and support rollout of training programs	• 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 the enterprise risk tolerance framework implementation • Provide input, review and agree on risk tolerances and underlying metrics proposed by risk management • Coordinate and consolidate the development of SHUSA risk tolerance • Deploy SHUSA risk tolerance statement	• Establish and maintain ERM policies aligned with the risk framework and risk tolerance • Review and opine on risk-relevant operating policies and procedures set by the first line of defense • Develop and allocate risk tolerance 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	• Challenge management on the appropriateness of 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

Monitoring, Testing and Reporting			
Line 1	**Line 2**		**Line 3**
Business Acts. / Corp. Functions	***ERM Program***	***Risk Management Areas***	***Internal Audit/Credit Risk Review***
• Manage Risk Taking Activity • Provide Quality Assurance for Line 1, including reconciliations of Results, Balance Sheet and activities • Execute Controls and Monitoring Protocols for Line 1 • Working with the Risk Model ERM function, define risk model usage, embed risk model ownership policies and procedures in Line 1 activities, define and implement Line 1 model documentation and controls • Prepare RTS underlying metrics (e.g. risk mandates) in coordination with Line 2 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 to evaluate the effectiveness of Incident Response Plans • Report on key, evolving and emerging risks • Report on RTS underlying metrics (e.g. risk mandates) • Report on Quality Assurance activity developed by Line 1 • Escalate identified deficiencies as well as audit findings, regulatory reviews, etc. • Report on status of Remediation Plans	• Aggregate, harmonize and consolidate risk MIS and other risk reporting at the SHUSA level and provide guidance/guidelines for underlying subsidiaries • Consolidate and Report on compliance with the risk framework at the SHUSA level • Coordinate, aggregate and correlate emerging and key risks • Establish and administer an ERM model risk function, coordinating all model risk activities across SHUSA and its subsidiaries • Escalate key issues and exposures to appropriate risk committees • Analyze and report on adequacy of consolidated limits • 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	• Establish a risk reporting framework which enables effective monitoring and reporting on risks within the lines of business • 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 function • Monitor and aggregate reporting on standards, limits and tolerances 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	• 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 tolerance • Evaluate the 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 and Audit Committee • Evaluate that management establishes effective remediation plans • Monitor corrective action and conduct follow-up reviews to ensure recommendations have been addressed ***Loan Review Function*** • 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

4.8 Risk Map vs Lines of Defense



Areas reporting to the CRO

5. SHUSA Risk Organization

5.1 Overview

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

5.2 Risk Management Function

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

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

5.3 The ERM Risk Managers

Overseeing Credit Risk, Market and Liquidity Risk, Operational Risk, Methodology Risk, Compliance Risk and Model Risk, the ERM Risk Managers are responsible for developing the ERM Risk Frameworks and related Policies for their risks, facilitating subsidiary implementation of the policies, overseeing the development of subsidiary operating policies and procedures, ensuring compliance with the related risk policies, and proposing, assessing, controlling, reporting and monitoring risk tolerances and limits for their respective risk areas.

Detailed roles and responsibilities for the risk managers, with respect to Identification and Assessment, Control and Monitoring, Testing and Reporting, for the relevant risk areas are to set forth in the appropriate ERM frameworks and Policies.

5.4 The Risk Architecture Function

Covering the areas of Governance and Control Processes, Risk Management Information (“MI”), Risk Identification (“ID”), Risk Aggregation and Control and Risk Tolerance, the Risk Architecture unit is responsible for the development and implementation of the ERM Framework and related risk policies, coordination of internal reporting to senior committees including the Board, project oversight for the ERM function, the ERM technology and data strategies (including the definition of systems requirements for the ERM function and the Risk Data Aggregation framework), the production of MI

including regulatory reporting, Risk ID, Risk Tolerance Statement, Risk Aggregation, Capital Planning, Stress Testing and the analysis and reporting of MI to the relevant committees and senior management.

5.5 SHUSA and Subsidiary Risk Management Organizations

Each SHUSA subsidiary will maintain its own risk management organization structure that reflects the SHUSA structure as applied to the subsidiary based on their business model, size and complexity. This will include both the risk management organization and the committee structures. Each subsidiary risk organization will report hierarchically to its respective board of directors and CRO through this risk management organization and committee structure. The subsidiary 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 subsidiary Chief Risk Officers to the SHUSA CRO and from the subsidiary risk officers to the respective SHUSA risk officers.

This structure is in place to maintain the integrity of SHUSA's individual subsidiaries, and the accountability of their boards of directors and of executive management for their performance. Through the defined control and reporting responsibilities of subsidiary 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 subsidiary.

6. ERM Frameworks, Policies and Procedures

6.1 Overview

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, and ensure a unified approach to the management of risks across SHUSA and its subsidiaries. Each of the Frameworks and Policies will set forth the respective roles and responsibilities for risk management by Line 1 and Line 2 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 subsidiaries. Subsidiaries are expected to adhere to the principles embodied in the SHUSA ERM Frameworks and Policies through the development of subsidiary frameworks and policies tailored to the specific needs of the subsidiary and aligned with the requirements of the SHUSA ERM Frameworks and Policies.

6.2 The policy hierarchy

The SHUSA policy hierarchy incudes ERM Policies, Operating Policies and Process and Administrative documents as depicted below:

	Location	Coverage	Policy Owner	Authority	Frequency
Enterprise Policies	SHUSA only	All SHUSA subsidiaries	SHUSA Executive Management	SHUSA Board	Annual
Operating Policies	All subsidiaries	Individual subsidiary	Subsidiary Executive Management	Subsidiary Board of Directors	Annual or 1-3 years on management certification
Process and Administrative Documents	All subsidiaries	Individual subsidiary	Functional Managers	Functional Heads	As needed

7. ERM Methodology

7.1 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.** These integrated processes apply to all risks and risk-types, and together form the core elements of the ERM Methodology. Each subsidiary is expected to adopt and execute upon this program consistent with the nature and complexity of its risks and activities. The principles that underpin the ERM Methodology are:

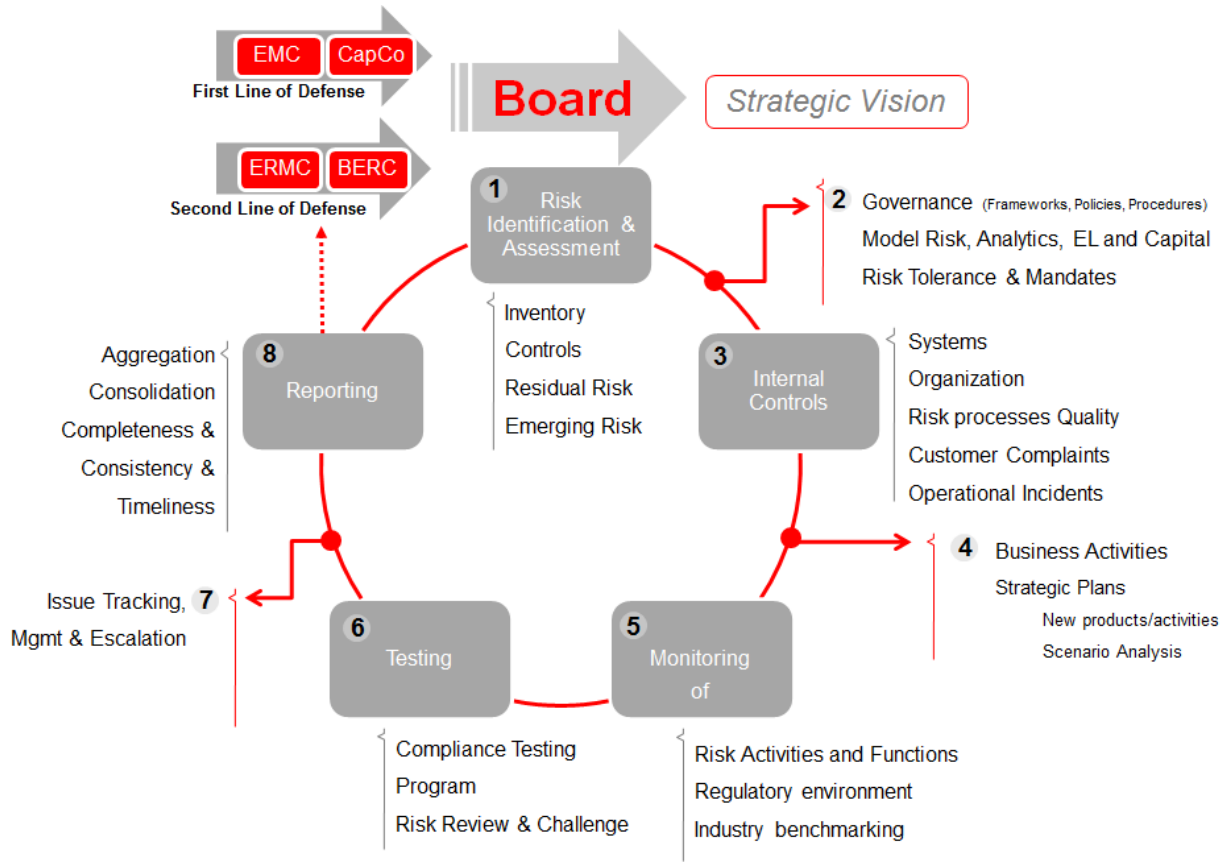
- **Risk identification** must be undertaken both at initiation of an activity and as an activity or the risks change with circumstances both internal and external to the organization.
- **Risk assessment** is the process by which all identified risks are measured for materiality. This process evaluates 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 operations of the SHUSA subsidiaries.

7.2 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[4]. All Frameworks and Policies must ensure that the ERM methodology is embedded across all risks and all the organization.

The hallmark of an ERM methodology 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.

[4] 'Cycle' denotes a conceptual relationship and not necessarily 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.



1 Risk ID and Assessment
• Risk Identification:
  ○ Risk inventory
  ○ Risk measurement
  ○ Risk quantification
  ○ Risk controls and mitigants
• Risk response – accept/ mitigate/ reject.
• Risk Correlation
• Emerging Risks
	2 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 tolerance & Mandates • Risk Tolerance Limits & Metrics • Risk Scoring, Risk Approvals & Mandates

3 Internal Control
• Quality assurance and Control
  ○ Systems
  ○ Organization
• Risk processes quality
• Customer complaints
• Operational incidents
	4 Business Activities
	• Business plans
	• Commercial strategy
	• New Products
	• Business plan scenario analysis

5 Monitoring • Regulatory, Policy and Business • Industry benchmarking • Risk Activities and functions • Risk Limits, KRIs, KPIs, Risk Tolerance Statement	**6 Testing** • Compliance Testing Program • Risk Review & Challenge
7 Issue tracking and Escalation	**8 Reporting** • Risk Monitoring / Loan Quality • Risk Reporting • Risk Aggregation / Consolidation • Completeness, consistency & timeliness • Regulatory Reporting

8. Document History and Version Control

8.1 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

8.2 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