Santander Holdings USA, Inc.

OPERATIONAL RISK MANAGEMENT FRAMEWORK

Table of Contents

1. Introduction

1.1 Background

The goal of the Santander Holdings USA, Inc. ("SHUSA" or "the Company") Operational Risk Management Program ("ORM Program" or "Program") is to manage operational risk in SHUSA-located operations ("subsidiaries") and enterprise-wide in a comprehensive, consistent and effective fashion, enabling the firm to achieve its strategic priorities consistent with its expressed risk tolerance. The identification, assessment, control, monitoring, testing and reporting of risks, together with the clear articulation and communication of risk appetite, provide the foundation of a strong ORM Program. This Operational Risk Management Framework ("ORM Framework" or "Framework") sets forth the SHUSA expectations for the consistent and effective management of operational risk in each subsidiary and at the enterprise level. SHUSA expects that managers at all levels will understand, embrace, implement and reinforce, within their organizations, prudent risk taking in line with this ORM Framework.

1.2 Scope

The SHUSA ORM Framework applies to SHUSA and its subsidiaries. SHUSA is a U.S. bank holding company with two main subsidiaries, Santander Bank, N.A. ("SBNA"), a national bank, and Santander Consumer USA Inc. ("SCUSA"), a public, non-bank consumer finance company that is majority-owned and controlled by SHUSA (together "subsidiary" or "subsidiaries" or the "organization").

This Framework describes the principles for the management, control and oversight of operational risk across SHUSA and its subsidiaries as U.S. regulated institutions.

The Company expects that managers at all levels will understand and embed within their organizations the prudent operational risk principles described in this Framework. Before being approved at the local level, Frameworks shall be submitted to SHUSA for validation in order to ensure consistency with this Framework.

1.3 Purpose of the Operational Risk Management Framework

The SHUSA Board has approved an overarching SHUSA Enterprise Risk Management Framework ("ERM Framework") that sets the principles of SHUSA's oversight of risks arising from its business activities and operations and governs its risk management activities. This ORM Framework must be read in conjunction with the SHUSA ERM Framework as its purpose is to develop the Enterprise Risk Management Program ("ERM Program") in relation to operational risk. This ORM Framework describes the operational risk management principles and governance that must be followed by SHUSA and its subsidiaries when identifying, managing, controlling and aggregating Operational Risks and is designed

to achieve consistent practices across the organization and in compliance with all applicable rules, regulations and guidance.

This Framework is aligned to the Operational Risk Framework approved by the Board of Directors of Banco Santander S.A. and that establishes the principles that must be followed by all Santander Group Subsidiaries when managing Operational Risk.

1.4 Document Ownership and Maintenance

As owner, the SHUSA Chief Risk Officer ("CRO") is responsible for the development and maintenance of this ORM Framework. The Chief Operational Risk Officer ("CORO") of SHUSA has primary responsibility for ensuring it is implemented and embedded on a day-to-day basis. The ORM Framework is approved by the SHUSA Enterprise Risk Management Committee ("ERMC") under recommendation from the SHUSA Operational Risk Management Committee ("ORMC").

The Framework is reviewed and amended by the ORMC as needed to ensure that it remains applicable to SHUSA's strategy and current and planned activities. Ad-hoc Framework reviews can be performed at the discretion of the CORO, CRO, or SHUSA Chief Executive Officer ("CEO"). The ERMC or the SHUSA Risk Committee may also initiate changes to the Framework in response to changing conditions. Changes or updates to the Framework must be developed in consultation with the CORO and CRO and approved by the ORMC.

2. Operational Risk and Other Risk Types

2.1 Definition of Operational Risk

SHUSA defines operational risk as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk.

Operational risk is inherent in all SHUSA products, activities, processes, and systems. As such, every employee, business process, and system has a role in the identification, management and control of operational risk.

SHUSA categorizes operational risk into seven risk event categories as follows:

Internal Fraud	The risk of losses from willful actions designed to defraud, misappropriate goods or evade business regulations, laws or policies (excluding diversity/discrimination events) in which at least one person linked to the company is implicated. Examples: misappropriation of assets, tax evasion, intentional mismarking of positions, bribery.
External Fraud	The risk of losses from willful actions designed to defraud, misappropriate goods or evade business regulations, by a third party separate from the company. Examples: theft of information, hacking damage, third-party theft and forgery.
Employment Practices & Workplace Safety	The risk of losses from actions that is incompatible with legislation or agreements on labor, health or safety. Indemnity payments for damage to people, or diversity/discrimination events. Examples: discrimination, workers compensation, employee health and safety.
Clients, Products & Business Practices	The risk of losses arising from accidental or negligent breaches of professional obligations with specific clients, (including fiduciary or suitability requirements), or from the nature or design of a product. Examples: market manipulation, antitrust, improper trade, product defects, fiduciary breaches, account churning.
Damage to Physical Assets	The risk of losses of non-budgeted value or costs in material assets, derived from damages produced by natural disasters or other external events. Examples: natural disasters, terrorism, vandalism.
Business Disruptions & System Failures	The risk of losses and compensation caused by disruption of business or systems malfunctions. Examples: utility disruptions, software failures, hardware failures.
Execution, Delivery & Process Management	The risk of losses arising from failed transaction processing or process management, from relationships with trade counterparties, suppliers and vendors. Examples: data entry errors, accounting errors, failed mandatory reporting, negligent loss of client assets.

3. Principles

3.1 Risk Culture and Risk Management Accountability

A strong risk management culture supports SHUSA's long term success. Through its Values Statement and Code of Conduct, the SHUSA Board of Directors ("SHUSA Board" or "Board") has communicated the values and behaviors it expects the staff of SHUSA and its subsidiaries to adopt in their daily activities.

As reflected in the ERM Framework, risk management accountability will be incorporated into all Frameworks and Policies at SHUSA and its subsidiaries. This accountability is evidenced through clear definitions of roles and responsibilities for risk management, the alignment of performance and compensation with risk management goals and the ongoing support that must be provided by senior management to ensure that sufficient and competent risk management resources are deployed throughout the organization and that appropriate risk training is provided to all staff as required.

3.2 Operational Risk Management Governance Principles

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

- **Integral Management of Operational Risk** – Through the effective implementation of the Enterprise Risk Management Methodology ("ERM Methodology"), SHUSA and its subsidiaries must, (1) develop, implement and maintain a consistent, documented Operational Risk Management ("ORM") program that ensures operational risks will be identified, measured, monitored and controlled in all products and business activities (including new products and services) and that, (2) operational risk policies and standards are being properly communicated, implemented, that they remain effective and appropriate and, (3) that operational risk decisions are being made taking into consideration a balanced measurement of risk and incentives and are considered in strategy planning. ORM programs must consider the differences in nature, size, complexity, and risk profile of each SHUSA subsidiary.

- **Independent Functions** – Although all team members are responsible for managing and controlling operational risks within their responsibility, the management function that originates operational risks in the business should be separate from the risk function that will execute the necessary controls over the risks incurred. Senior management must develop a clear, effective and robust ORM governance structure with well-defined, transparent and consistent lines of responsibility.

- **Independent Structure** – The SHUSA Board and the subsidiary boards will ensure the development and maintenance of independent operational risk management functions and operational risk governance structures that are communicated and understood throughout the organization. Effective operational risk reporting is required and is the means by which the SHUSA Board, its management committees and all other governance structures are informed of the operational risks and issues identified in the operations of SHUSA and its subsidiaries.

- **Control Environment -** Senior Management must have a strong control environment that utilizes policies, processes, procedures and systems, appropriate internal controls, and appropriate risk mitigation and/or transfer strategies.

- **Consolidated View of the Risks Taken** – A consolidated view of all the operational risks incurred by SHUSA and its subsidiaries in the course of their businesses must be available, so that operational risk management and reporting is effective, efficient and homogeneous. This consolidation will be aligned to the reporting requirements of Santander S.A. by using common tools, taxonomies and metrics subject to agreed dispensation.

- **Defined Authority** – The SHUSA Board and the subsidiary boards will ensure that the operational risk management teams establish separate and focused governance processes including committees and delegated authorities to oversee the operations of their function at the level of SHUSA and its subsidiaries.

- **Definition of Limits** – The SHUSA operational risk management function will work with the subsidiary operational risk management functions to define operational risk limits for each subsidiary and business line as appropriate by type of activities, segments and products. These limits will be expressly reviewed and approved by the applicable Board at least once a year or whenever there are significant variations in the risk profile of SHUSA or its subsidiaries. The limits will be subject to consolidation at SHUSA and Santander S.A. level to ensure that they can be measured and controlled and that they remain within the approved risk tolerance for each entity. Operational risk limits are used in the strategic business planning process to better facilitate the analysis of risk versus return and to improve decision-making.

- **Clear Oversight and Escalation Processes** – Operational risk governance and escalation policies will ensure that responsibility for oversight and reporting of operational risk and the rules and processes for escalating issues are understood and followed throughout the organization. Any significant breach or weakness identified at any level of the subsidiaries must be promptly escalated to the subsidiaries' CORO and to the SHUSA CORO who will review and recommend actions to address the issues and emerging risks and ensure that the subsidiaries implement the recommendations. Examples of issues that may be escalated include limit breaches, regulatory matters or internal audit recommendations. If the recommended actions are not followed, the SHUSA CORO will escalate the matter to the SHUSA CRO and the ORMC, ERMC, RC and Board if appropriate.

- **Contingency Plans and Technical Capability** – SHUSA and its subsidiaries should have contingency plans in place to ensure that their day-to-day operational risk management activities are not disrupted under exceptional circumstances. These plans should be adequately resourced from both a technical and a staffing perspective**.**

- **Training and Awareness** – Periodic operational risk awareness training is required of all employees, tailored to employees' roles in operational risk management. With oversight from SHUSA Operational Risk Management, subsidiaries will identify training needs and develop training programs.

- **Risk and Compensation** – The objective setting, performance management and compensation programs must be aligned to operational risk management objectives. To be considered properly functioning programs, they must avoid incentivizing inappropriate risk taking activities. Performance against operational risk objectives must be appraised, documented and linked, where appropriate, to quantitative measures.

- **Internal/External Communication –** Operational risk related communication for public purposes or for reporting to regulatory agencies will take place in accordance with regulatory requirements and in line with SHUSA Regulatory Communications Protocols.

- **Review and Challenge** – Management review and challenge processes are required to be established as part of the operational risk governance structures to ensure adequate oversight of operational risk-taking and risk management activities. Management review and challenge includes dedicated oversight and review by an independent operational risk control function, the RC and Board where applicable, and an internal audit function vested with appropriate stature and authority.

4. Elements of the Operational Risk Management Program

The objective of the ORM Program is to enable SHUSA to comprehensively identify, assess, mitigate, measure, report and manage operational risks. SHUSA and its subsidiaries must develop, implement and maintain a documented ORM Program that is fully integrated into SHUSA's overall risk management processes. On a periodic basis, at least annually, an evaluation must be completed to ensure all new and existing subsidiaries and its' material business units and business lines are included. The ORM Program is comprised of five elements:

1. Policy and Governance

It is the policy of SHUSA to manage operational losses and exposures within the limits of the approved tolerance for operational risk, capitalize its operational risk exposures appropriately and in compliance with regulatory requirements, honor its commitments to customers, communities, and shareholders, and maintain a strong and adequately resourced ORM function consistent with achieving these objectives.

a. **Operational Risk Appetite** – SHUSA must manage operational risk within specific operational risk limits as defined in SHUSA Risk Appetite Statement and Subsidiary risk appetite statements. The operational risk appetite consists of qualitative and

quantitative measures and standards which enable SHUSA and its Subsidiaries to evaluate operational risk exposures.

b. **Training and Awareness** – Annual Operational Risk Awareness Training is required of all employees. SHUSA and its Subsidiaries will provide periodic ad-hoc training as appropriate.

c. **Quality Assurance** – SHUSA and its Subsidiaries will utilize a quality assurance process to ensure program implementation in the business lines and support functions as appropriate.

2. Assessment and Issue Management

a. **Risk and Control Self-Assessment** – SHUSA and its Subsidiaries will employ a Risk and Control Self-Assessment "RCSA" for the business to identify and assess operational risks that are inherent in their material business processes. Additionally, the business must identify, document and assess the effectiveness of the key internal controls in place to mitigate those risks. The RCSA must be conducted at least annually.

b. **Scenario Analysis** – SHUSA and its Subsidiaries must conduct a Scenario Analysis exercise on an annual basis. Scenario analysis is a forward-looking exercise to obtain exceptional but plausible severity estimates of operational risk losses.

c. **Operational Risk Issue Management and Mitigation** – SHUSA and its Subsidiaries must have an effective operational risk management program that will assist in identifying issues that require corrective action or resolution. The capture, tracking and oversight of issues are critical to ensuring proper resolution and closure.

3. Loss Data

a. **Internal Operational Risk Loss Event Data** – A consistent and robust process for collection of internal loss data is critical to the SHUSA's ability to measure and manage operational risk effectively. SHUSA and its Subsidiaries must ensure that they have robust processes for the collection and use of its loss data.

b. **External Operational Loss Data** – External Operational Loss data are loss events that are publicly reported losses that have occurred at other financial institutions. Consideration of external loss data events is a required element of the Basel II Advanced Measurement Approach.

4. Monitoring and Reporting

a. **Monitoring and Reporting** – SHUSA and its Subsidiaries must define risk monitoring and reporting mechanisms to ensure appropriate communication of operational risk information to all interested parties.

b. **Operational Risk Event Escalation, Monitoring and Reporting** – Effective operational risk event escalation and monitoring processes are critical to ensure proper mitigation and resolution of material and significant events. SHUSA and its Subsidiaries must have operational risk event escalation and monitoring processes that are designed to meet the SHUSA requirements at a minimum.

c. **Key Risk Indicators** – SHUSA and its Subsidiaries use Key Risk Indicators ("KRIs") to identify, measure, monitor and control aggregate operational risk in relation to SHUSAs Board approved Risk Tolerance Statement. Specific KRIs are developed and used to ensure that operational risk levels and limits are within Board approved risk tolerances. Corrective actions to reduce the operational risk levels, or risk acceptance of elevated operational risk levels may be necessary.

5. **Loss Forecasting / Capital Modeling** – Capital modeling is a key factor in determining SHUSA's regulatory capital requirements. SHUSA and its Subsidiaries provide critical information needed to complete this process.

See the SHUSA Enterprise Operational Risk Management Policy for further definitions and roles and responsibilities.

5. Three Lines of Defense

SHUSA and its subsidiaries 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 ("First Line of Defense" or "1st LOD") Risk Management – SHUSA, its subsidiaries and their Lines of Business & Lines of Business Support Units: reporting to the Chief Executive Officer ("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 ("Second Line of Defense" or "2nd LOD") 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 and provides legal expertise and support when operational risk events have potential civil or criminal consequences including litigation.

- Line 3 ("Third Line of Defense" or "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 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.

6. SHUSA Operational Risk Management Roles and Responsibilities

6.1 SHUSA Ownership Structure

SHUSA is wholly owned by Banco Santander, S.A. ("Santander" or the "Group").

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 operational risks and operational risk management activities to Santander S.A.

6.2 The SHUSA Board of Directors

The SHUSA Board is responsible for SHUSA's oversight.

With respect to governance, implementation, and monitoring of the ORM Framework, the SHUSA Board has delegated its responsibilities to the SHUSA Enterprise Risk Management Committee which will review and approve the Framework and oversee implementation of the ORM Framework and monitor compliance.

6.3 The SHUSA Chief Executive Officer

The Board delegates full responsibility to the SHUSA Chief Executive Officer ("CEO") for the execution of business activities including the front line management of risks on a day-to-day basis.

The main responsibilities of the CEO are detailed in the ERM Framework and they include, among others, the management of operational risk arising from the agreed strategy and business plan, proposing the operational risk tolerance statement, delegating authority to the Subsidiary CEOs, overseeing the establishment of appropriate systems and controls, reporting to the Board and ensuring an appropriate risk culture.

6.4 The SHUSA Chief Risk Officer

The SHUSA Chief Risk Officer ("CRO") is an independent executive who reports to the SHUSA Risk Committee and the CEO.

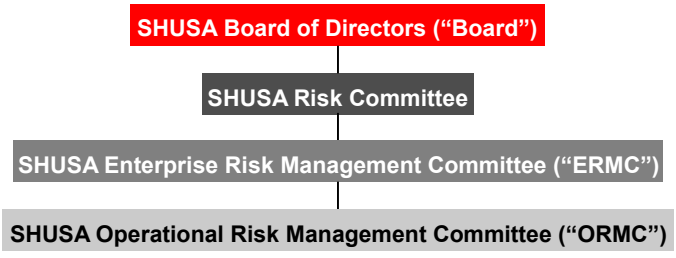
The CRO's responsibilities are detailed in the ERM Framework and they include, among others, implementing the SHUSA ERM Program and overseeing the management and control of operational risk within the parameters of the ERM Program; reviewing, challenging and controlling the operational Risk Appetite; and reporting operational risk management deficiencies including escalation of breaches through the Committee process.

On a day-to-day basis, the CRO delegates his operational risk ERM responsibilities to the SHUSA CORO whose responsibilities are detailed in Section 6.6 of this Framework.

6.5 Key Operational Risk Management Committees

SHUSA implements its risk 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.

The SHUSA Operational Risk Management Committee and its reporting structure are reflected in the diagram below and its subsidiaries must adopt and adapt this structure when establishing their independent governance and decision-making bodies and defining their charters.



6.5.1 The SHUSA Risk Committee

The SHUSA Risk Committee is appointed by the SHUSA Board to assist it in its oversight responsibilities with respect to enterprise risk management activities and related compliance matters.

6.5.2 The SHUSA Enterprise Risk Management Committee

The ERMC is established under the authority of the RC and it 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.

6.5.3 The SHUSA Operational Risk Management Committee

The ERMC and CRO established the ORMC to oversee operational risk. ORMC has primary responsibility to oversee and manage the identification and monitoring of operational risk in SHUSA and its subsidiaries. The ORMC advises the ERMC and subsidiary board committees on the supervision, control and reporting of the operational risks related to subsidiary operations and activities.

6.6 SHUSA Chief Operational Risk Officer

The SHUSA Chief Operational Risk Officer ("CORO") is responsible for the day-to-day management of Line 2 ERM responsibilities at SHUSA as described above, as well as for the coordination and supervision of the Line 2 Risk Management functions in the subsidiaries.

The CORO, in agreement with the subsidiary CRO, will:

- Participate in the decision to hire or dismiss subsidiary COROs
- Set goals and objectives for subsidiary COROs
- Contribute to the annual performance evaluations of subsidiary COROs
- Participate in compensation decisions regarding subsidiary COROs

The CORO:

- Leads the SHUSA ORM program across subsidiaries, providing for effective supervision of all operational risks and operating independently from the subsidiaries and their business lines.
- Ensures that SHUSA´s ORMC and other senior management committees are informed and are able to discharge their responsibilities according to their charters.
- Is the model owner for all Operational Risk loss forecasting models.

6.7 SHUSA Operational Risk Management Function

SHUSA Operational Risk Management includes officers responsible for overseeing the core operational risk management areas: Operational Risk, Information Risk, Third Party Provider Risk and Business Continuity Management. In each of these areas, the officers own the Enterprise Policies and Standards for their risk areas, facilitate subsidiary implementation of the policies and standards, oversee the development of subsidiary operating policies and procedures, and oversee compliance with the policies and standards for their respective risk areas.

7. Document Administration

7.1 Ownership and Authorship

Version	Date	Author	Owner	Change
1.0	10-1-2015	SHUSA CORO	SHUSA CORO	

7.2 Sign Off

Approving Body	Governance Committee Approval or Endorsement	Final Approval Date
SHUSA ERMC	SHUSA ORMC	12-04-2015

8. Appendix – Regulatory Guidance as of 9/11/2014

#	Category	Guidance
1	Basel Guidance	Basel Committee on Banking Supervision (BSBS) - Principles for the Sound Management of Operational Risk
2	Basel Guidance	Basel Committee - Principles for effective risk data aggregation and risk reporting
3	Interagency Guidance	Board of Governors of the Federal Reserve System, FDIC, OCC, OTS - Interagency Guidance on the Advance Measurement Approaches for Operational Risk
4	Federal Reserve Bank Guidance	FRB Capital Planning at Large Bank Holding Companies: Supervisory Expectations and Range of Current Practice
5	Federal Reserve Bank Guidance	FRB Enhanced Prudential Standards
6	Office of the Comptroller of the Currency Guidance	Final Rules and guidelines - OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of Regulations