Santander Holdings USA

ENTERPRISE OPERATIONAL RISK MANAGEMENT POLICY

Santander Holdings USA ("SHUSA") believes that our success is grounded in our values. Santander's commitment to treat customers, colleagues and stakeholders in a manner that is *Simple, Personal, and Fair* means that our every action is founded on *INTEGRITY, CUSTOMER COMMITMENT, PEOPLE, TEAMWORK, OWNERSHIP,* and *INNOVATION*. It is because of this commitment that our customers and clients trust us to deliver world class products and services and select Santander to be their bank of choice. Safeguarding this trust – by always conducting business responsibly, with integrity and a disciplined approach to risk management – is a responsibility shared by each Santander Team Member.

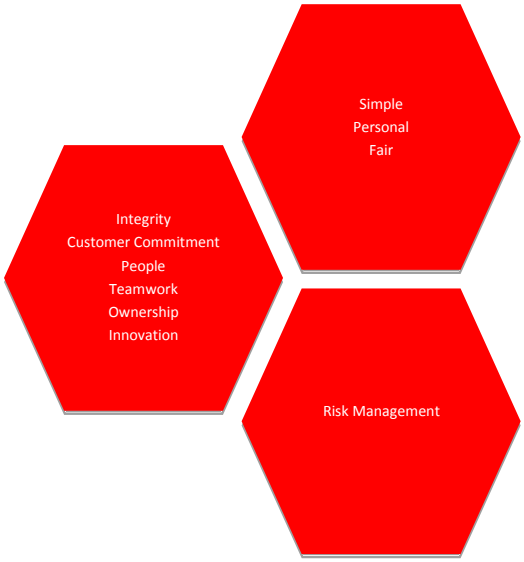

Table of Contents

1 Introduction

1.1 Purpose of the Document

The purpose of the Santander Holdings USA, Inc. ("SHUSA") Operational Risk Management Enterprise Policy ("Policy") is to govern the establishment and operation of SHUSA's program for managing operational risk. Operational risk is inherent in all of SHUSA's products, activities, processes and systems. The adequate and effective identification, assessment, control, monitoring, testing and reporting of operational risk within the risk appetite, reviewed and confirmed by the SHUSA Board of Directors ("the Board") is a fundamental element of SHUSA's Operational Risk Management ("ORM") program.

This Policy aligns with the overall enterprise risk management strategy and should be reviewed in conjunction with the SHUSA Enterprise Risk Management Framework.

1.2 Scope

This Policy applies to SHUSA and its Subsidiaries, including but not limited to Santander Bank, N.A. ("SBNA") and Santander Consumer USA, Inc. ("SCUSA"). Policies developed by the Subsidiaries must comply with the requirements set forth in this Policy.

This Policy replaces the following policies:

- SHUSA Operational Risk Mitigation Policy
- SHUSA Operational Risk Incident/Event Identification and Escalation Policy
- SHUSA Operational Risk Assessment Policy
- SHUSA Operational Risk Key Risk and Early Warning Indicator Policy
- SHUSA Operational Risk Scenario Policy
- SHUSA Operational Risk Loss, Near Miss and Event Data Collection Policy

The aforementioned policies will be retired as of the approval date of this Policy. The content of these items has been captured within this Policy or in the applicable standards.

1.3 Document Approval and Maintenance

The SHUSA Chief Operational Risk Officer ("CORO") has primary responsibility for the ownership, oversight, development, issuance and maintenance of this Policy. The SHUSA CORO will ensure that this Policy complies with applicable laws, regulations, and guidelines and is updated to reflect the current operating environment. This Policy is reviewed and recommended by the SHUSA Risk Committee for final presentation to and approval by the SHUSA Board on an annual basis.

This Policy is reviewed and, if necessary, updated at least annually, or when changes occur, to ensure the Policy aligns to regulatory requirements and SHUSA's strategy and current and planned activities. Ad-hoc reviews and

updates may be made to this Policy at the discretion of the SHUSA Chief Risk Officer ("CRO"), SHUSA Enterprise Risk Management Committee ("ERMC"), SHUSA Risk Committee, or SHUSA Board based on changes in business operations, audit recommendations, and/or testing results. Changes or updates to this Policy must be developed in consultation with the SHUSA CORO. All material changes must be approved by the SHUSA Board.

1.4 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, mandated and defined in the SHUSA Operational Risk Management Framework and this Policy, which 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
2. Assessment and Issue Management
3. Loss Data
4. Monitoring and Reporting
5. Loss Forecasting / Capital Modeling

1.5 Types 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.

SHUSA categorizes operational risk into seven risk event categories as defined by the following regulatory guidance:

- Basel Committee on Banking Supervision ("BCBS") – Principles for the Sound Management of Operational Risk (June 2011)
- Board of Governors of the Federal Reserve System, FDIC, OCC, OTS – Interagency Guidance on the Advanced Measurement Approaches for Operational Risk (June 3, 2011)

The seven operational loss event categories are 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.

2 Governance and Accountability

2.1 SHUSA Governance

This Policy is governed by the following committee structure:

The full responsibilities of the SHUSA Board are detailed in its bylaws and committee charters. With respect to this Policy, the SHUSA Board is responsible for the following:

- Establishes the Policy,
- Reviews and approves the Policy,
- Oversees implementation of the Policy,
- Monitors compliance with the Policy,
- Monitors exceptions to the Policy, and
- Ensures annual review and approval of the Policy.

The SHUSA Risk Committee reviews and recommends this Policy to the SHUSA Board for approval on an annual basis or on a frequency as otherwise mandated by the Policy.

The ERMC recommends this Policy to the SHUSA Risk Committee for approval on an annual basis or on a frequency as otherwise mandated by the Policy.

The SHUSA Operational Risk Management Committee ("ORMC") reviews this Policy, oversees updates to it as necessary, provides input regarding significant changes and oversees consistency across SHUSA and its Subsidiaries.

3 Policy

3.1 Policy Statement

It is the policy of SHUSA to manage operational losses and exposures within the limits of the approved appetite 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.

Operational risks must be considered by senior management within their strategic planning process and in their decision making.

Note: Where appropriate, standards and other process and administrative documents have been created to support the requirements within this Policy. Standards related to this Policy are maintained by SHUSA Operational Risk Management ("ORM"). Please see the Appendix section for a listing of related policies and procedures.

3.1.1 Operational Risk Appetite

SHUSA must manage operational risk within specific operational risk limits as defined in SHUSA 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.

Requirement	Accountable Unit(s)
1. SHUSA and its Subsidiaries must implement an ORM Program to manage operational risk within the approved operational risk appetite and loss budgets. The SHUSA Board, SHUSA Risk Committee and SHUSA ERMC must receive regular reporting on the level of operational risk exposures relative to the approved risk tolerance**.**	1st Line – Subsidiaries 2nd Line - Subsidiaries 2nd Line – SHUSA
2. For any breaches in the risk appetite metrics, escalate in line with SHUSA governance and provide mitigation plans designed to bring the metric back within the established limits.	1st Line – Subsidiaries
3. Develops and allocates operational risk appetite limits for SHUSA and its Subsidiaries and provides input on underlying risk metrics	2nd Line – SHUSA

3.1.2 Training and Communication

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

Requirement	Accountable Unit(s)
1. Ensure training programs and sessions are completed and or attended as intended	1st Line – Subsidiaries
2. Create, develop and refresh programs and inventory for Operational Risk training and awareness and communicate as necessary	2nd Line – Subsidiaries 2nd Line – SHUSA

3.1.3 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.

Requirement	Accountable Unit(s)
1. Develop quality assurance* and use-testing processes to evaluate the effectiveness of the Operational Risk Management Program	2nd Line – Subsidiaries 2nd Line - SHUSA
2. Conducts independent verification of compliance with the SHUSA operational risk framework, policies and standards across the Subsidiaries	2nd Line – SHUSA

* Quality assurance will include an evaluation of business line, control functions and Risk Management areas. Testing of controls, or review of 1st Line control testing, will be done on a sample basis.

3.2 Assessment and Issue Management

3.2.1 Risk and Control Self-Assessment ("RCSA")

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.

Requirement	Accountable Unit(s)
1. Develop and maintain the RCSA Methodology Standard, which includes taxonomies, rating scales, relevant templates, etc.	2nd Line – SHUSA
2. Execute the RCSA in accordance with the RCSA Methodology Standard	1st Line – Subsidiaries
3. Business environment and internal control factors "BEICF", such as KRIs, information from internal and external audits and regulators, etc. are to be leveraged as part of the assessments.	1st Line – Subsidiaries
4. Review and challenge the content captured within the RCSA. Escalate and report any unresolved challenges, as needed	2nd Line – Subsidiaries
5. Aggregate RCSA results and report to necessary functional areas including business line management and CORO	1st & 2nd Line - Subsidiaries 2nd Line – SHUSA
6. Develop and execute testing of key internal controls identified within RCSA	1st Line – Subsidiaries

3.2.2 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.

Requirement	Accountable Unit(s)
1. Provide a standardized Scenario Analysis methodology / standards to SHUSA and its Subsidiaries that include taxonomies and templates.	2nd Line – SHUSA
2. In conjunction with the Subsidiary 2nd LOD, coordinate scenario analysis development, ensures coverage of relevant risks, reviews process, perform assessment to ensure regulatory requirements are met	2nd Line – SHUSA
3. Oversee the scenario analysis workshops, reduce bias and ensure proper engagement of required subject matter experts relative to scenario being considered	2nd Line – Subsidiaries
4. Include appropriate subject matter experts relative to scenario	1st Line – Subsidiaries
5. Provide appropriate input and challenges during workshop and post workshop takeaways and maintain scenario analysis inventory	2nd Line – Subsidiaries 2nd Line – SHUSA
6. If output of analysis warrants follow-up actions ensure appropriate steps are taken and completed	1st & 2nd Line – Subsidiaries
7. Report results of analysis to appropriate management and to operational risk modeling team	1st & 2nd Line – Subsidiaries

3.2.3 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.

Requirement	Accountable Unit(s)
1. Establish and maintain a process to capture, track, mitigate (includes accepting, reducing, or transferring (i.e. insurance) risks) or respond to issues as they are identified	1st Line – Subsidiaries
2. Monitor issues/risk response, and where appropriate challenge, the status of progress or resolution of issues	2nd Line – Subsidiaries
3. Aggregate and report status of operational risk issues to the appropriate management routines and committees	2nd Line – Subsidiaries
4. Provide SHUSA and its Subsidiaries with issue management and mitigation	2nd Line – SHUSA

standards to further define expectations	
5. Oversees operational risk issues and remediation tracking, monitoring and escalation across the Subsidiaries	2nd Line – SHUSA

3.3 Loss Data

3.3.1 Internal Operational Risk Loss Event Data

A consistent and robust process for collection of internal loss data is critical to 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.

Requirement	Accountable Unit(s)
1. Designate a central repository for loss event capture	2nd Line – Subsidiaries
2. Identify, capture and report operational risk events in accordance with standards monthly	1st Line – Subsidiaries
3. Upload collected and reconciled data into central operational risk loss event repository monthly	2nd Line – Subsidiaries
4. Create and maintain business line procedures for identifying, capturing and reporting operational risk loss event data to the 2nd line of defense	1st Line – Subsidiaries
5. Perform root cause analysis on loss events that meet defined thresholds	1st Line – Subsidiaries
6. Attest to loss event data quality on a monthly basis	1st Line – Subsidiaries
7. Perform data quality checks, proper risk classification and data aggregation	2nd Line – Subsidiaries
8. Prepare internal operational risk loss event data and report as appropriate to support operational risk modeling and other corporate and regulatory reporting requirements	2nd Line – Subsidiaries
9. Provide SHUSA and its Subsidiaries with a standardized loss data collection methodology that includes taxonomies, required data fields, and relevant templates	2nd Line – SHUSA

3.3.2 External Operational Loss Data

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

Requirement	Accountable Unit(s)

1. Identify, capture and provide publicly reported external loss events to the business units	2nd Line – Subsidiaries
2. Review events provided and consider applicability in consideration of internal processes, controls and other relevant factors	1st Line – Subsidiaries
3. As required, ensure external loss data is included in the operational risk capital / loss forecasting models	2nd Line – SHUSA

3.4 Monitoring and Reporting

3.4.1 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.

1. Monitor and report operational risk exposures and information to management and 2nd Line	1st Line – Subsidiaries
2. Escalate key operational risk exposures to SHUSA, Subsidiary Management and Boards in a timely manner	2nd Line – Subsidiaries
3. Escalate key operational risk exposures in line with Corporate (Banco Santander, S.A.) reporting requirements	2nd Line – SHUSA
4. Provide information needed to customers, shareholders, consortiums, regulators and the general public in accordance with established requirements and protocols	2nd Line – Subsidiaries 2nd Line – SHUSA
5. Provide monitoring and reporting standards, including appropriate templates, to ensure consistent and accurate reporting across SHUSA and its Subsidiaries	2nd Line – SHUSA

3.4.2 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.

Requirement	Accountable Unit(s)
1. Identify and escalate operational risk events (“OREs”) that meet event thresholds set by ORM	1st Line – Subsidiaries
2. Develop action plans that mitigate and resolve escalated events and complete action plans in timelines set forth	1st Line – Subsidiaries

3. Report and escalate OREs in line with Corporate standards/procedures	2nd Line – Subsidiaries
4. Record escalated events in central repository within the month they are reported	2nd Line – Subsidiaries
5. Monitor escalated events through completion and provide reporting as required by SHUSA standards	2nd Line – Subsidiaries
6. Provide SHUSA and its Subsidiaries with standards that provide further guidance for escalating OREs	2nd Line – SHUSA
7. Escalates OREs in line with Group standards/procedures	2nd Line – SHUSA

3.4.3 Key Risk Indicators

SHUSA and its Subsidiaries use Key Risk Indicators ("KRIs") to identify, measure, monitor and control aggregate operational risk in relation to the SHUSAs Board approved Risk Appetite 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.

Requirement	Accountable Unit(s)
1. Develop, approve and monitor business line KRIs including triggers and limits	1st Line – Subsidiaries
2. If trigger or limit is breached take appropriate action and escalate to applicable areas	1st Line – Subsidiaries
3. In conjunction with the 1st Line, develop, approve and monitor standard SHUSA ORM KRIs	2nd Line – Subsidiaries
4. Monitor and report KRI breaches and subsequent mitigation plans for 1st line and ORM KRIs to ensure timely and successful resolution	2nd Line – Subsidiaries
5. Defines operational risk monitoring and reporting requirements which enables effective monitoring and reporting on risks (including KRIs, risk tolerance limits and mandates, top, emerging or evolving risks, etc.)	2nd Line – SHUSA

3.5 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.

Requirement	Accountable Unit(s)
1. SHUSA ORM must semi-annually coordinate with SHUSA Finance to calculate operational risk capital and feed the results into SHUSA's Capital Planning process	2nd Line – SHUSA

4 Roles and Responsibilities

4.1 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**

  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.

4.2 SHUSA Chief Operational Risk Officer

As part of the 2nd LOD, the SHUSA CORO is the overall owner of this Policy. Changes or updates to the Policy are developed in consultation with the CORO. The SHUSA CORO is responsible for maintaining the Policy and

managing and tracking exceptions to it.

4.3 Internal Audit

In their role as the 3rd LOD, Internal Audit conducts independent assessments of compliance with this Policy and related standards across SHUSA.

4.4 SHUSA Board of Directors

The SHUSA Board is responsible for overseeing the development, implementation, and maintenance of SHUSA's ORM Program. The SHUSA Board must ensure that this Policy is followed by all lines of business and corporate functions across SHUSA and must review and approve the Policy annually. The SHUSA Board must ensure necessary resources and funding are allocated to support the Policy.

4.5 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. In particular, and with regard to operational risk, the SHUSA Risk Committee reviews and recommends to the SHUSA Board policies and/or procedures for the identification, measurement and control, of operational risk as well as decisions to reduce, increase, transfer and/or hedge, operational risks in each Subsidiary.

4.6 SHUSA Enterprise Risk Management Committee

The ERMC is established under the authority of the SHUSA Risk Committee and is chaired by the SHUSA CRO. The ERMC is responsible for the oversight and monitoring of all risk-taking and risk management activities across the organization. The ERMC recommends this Policy to the SHUSA Risk Committee for approval on an annual basis or on a frequency as otherwise mandated by the Policy.

4.7 SHUSA Operational Risk Management Committee

The ERMC and CRO established the ORMC to oversee operational risk. The ORMC has the 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 operational risks related to Subsidiary operations and activities. The ORMC oversees adherence to the Policy across the organization.

4.8 SHUSA Chief Risk Officer

Ad-hoc reviews of this Policy can be performed at the discretion of the SHUSA CRO.

5 Reporting Structure

5.1 Reporting Structure

The SHUSA Head of ORM provides oversight, ensures effective controls, and implements an integrated enterprise-wide ORM Policy and Standards through coordination with the operational risk leads within SHUSA and each Subsidiary. The SHUSA Head of ORM reviews and reports on the status of Subsidiary operational risk to the SHUSA CORO. The SHUSA Head of ORM monitors, reviews and approves the metrics results and event reports and escalates the status to the SHUSA CORO.

6 Implementation, Enforcement and Exceptions

6.1 Policy Implementation

This Policy is effective immediately. It is understood that SHUSA and its Subsidiaries will require time to come into full compliance with this Policy. SHUSA Subsidiaries must evaluate the level of existing compliance with this Policy and, where necessary, develop a compliance implementation plan to achieve full compliance within one year in accordance with the SHUSA Operational Risk Management project plan.

SHUSA CORO will monitor SHUSA ORM's progress implementing this Policy and will update the SHUSA CRO quarterly until implementation is completed.

6.2 Policy Enforcement

This Policy is enforced by the SHUSA Risk Committee with the help of the Policy Owner. All violations of this Policy may result in penalties for the parties involved. Penalties may include:

- Re-training on Policy requirements
- Suspension or termination of employment, to the extent authorized by other published policies and procedures
- Suspension or termination of contract computer and/or network services

6.3 Policy Exceptions

Compliance with this Policy is mandatory. If a Subsidiary cannot comply with one or more of the requirements detailed within this Policy, an exception must be obtained. Exceptions from the Policy must be documented, indicating the rationale (constraints, objectives, compensating controls), expiration date for the exception, and the related risk(s). Exceptions are reviewed on a case-by-case basis and approved by SHUSA Management, SHUSA CORO, and SHUSA CRO. Documentation must be maintained by the SHUSA Operational Risk Management and will be included to the ORMC, ERMC, SHUSA Risk Committee and/or the SHUSA Board.

7 Document History and Version Control

7.1 Ownership and Authorship

Version	Date	Author	Owner	Change
Version 1	April 30, 2014	Head of Operational Risk Policy and Methodology	SHUSA CORO	
Version 2	September 15, 2015	Interim SHUSA CORO	SHUSA CORO	Aligned with SHUSA Enterprise Policy Administration Policy

7.2 Sign Off

Approving Body	Governance Committee Approval or Endorsement	Final Approval Date
SHUSA Board	SHUSA Risk Committee	December 2015
	ERMC	November 2015
	ORMC	October 2015

8 Appendices

8.1 Appendix A – Key Contacts

Title	*Role*	*Name and Contact*
Chief Operational Risk Officer	Policy Owner	Michael Lima, mlima1@santander.us
Head of Operational Risk	Primary point of contact on policy related matters	TBD
Director of Operational Risk	Secondary point of contact on policy related matters	TBD

8.2 Appendix B – Regulatory Obligations Addressed by this Policy

Regulatory Agency	Citation	Title
Basel Guidance	http://www.bis.org/publ/bcbs195.pdf	Basel Committee on Banking Supervision (BCBS) - Principles for the Sound Management of Operational Risk
Basel Guidance	http://www.bis.org/publ/bcbs239.pdf	Basel Committee - Principles for effective risk data aggregation and risk reporting
Interagency Guidance	http://www.federalreserve.gov/bankinforeg/srletters/sr1108a1.pdf	Board of Governors of the Federal Reserve System, FDIC, OCC, OTS - Interagency Guidance on the Advanced Measurement Approaches for Operational Risk
Federal Reserve Bank Guidance	http://www.federalreserve.gov/bankinforeg/bcreg20130819a1.pdf	FRB Capital Planning at Large Bank Holding Companies: Supervisory Expectations and Range of Current Practice
Federal Reserve Bank Guidance	12 CFR Part 252	FRB Enhanced Prudential Standards
Office of the Comptroller of the Currency	12 CFR Parts 30 and 170	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

8.3 Appendix C – Related Policies and Process and Administrative Documents

Document Type	Entity and Department	Owner	Document Title
Standard	SHUSA ORM	Chief Operational Risk Officer	SHUSA Operational Risk Issue Management and Mitigation Standard
Standard	SHUSA ORM	Chief Operational Risk Officer	SHUSA Operational Risk Internal Loss Data Collection Standard
Standard	SHUSA ORM	Chief Operational Risk Officer	SHUSA Operational Risk Quality Assurance Standard
Standard	SHUSA ORM	Chief Operational Risk Officer	SHUSA Risk & Control Self-Assessment Standard
Standard	SHUSA ORM	Chief Operational Risk Officer	SHUSA Operational Risk Event Escalation Standard
Standard	SHUSA ORM	Chief Operational Risk Officer	SHUSA Operational Risk Key Risk Indicator Standard
Standard	SHUSA ORM	Chief Operational Risk Officer	SHUSA Operational Risk Scenario Analysis Standard
Standard	SHUSA ORM	Chief Operational Risk Officer	SHUSA Operational Risk External Loss Data Standard