Santander Holdings USA

RISK APPETITE METRICS:
MONITORING, REPORTING, BREACH ESCALATION AND REMEDIATION PROCEDURE

Table of Contents

1. Introduction

1.1 Document Purpose

The Santander Holdings USA, Inc. ("SHUSA") Risk Appetite ("RA") metrics monitoring, reporting, breach escalation and remediation procedure (this "procedure document" or "document") defines the process through which the SHUSA Board of Directors ("Board")-approved risk appetite metrics are monitored and reported, and how triggers and breaches are identified, escalated, and remediated. It establishes the relevant roles and responsibilities, timelines, and documentation requirements that must be followed by the metric owners and Risk Managers for the correct monitoring of Board-level risk appetite metrics.

This document must be read in conjunction with SHUSA Risk Appetite Framework ("RAF"), the SHUSA Risk Appetite Statement ("RAS") and the SHUSA Risk Appetite Metrics Glossary[1].

1.2 Scope

This document applies to SHUSA and its subsidiaries. SHUSA expects its subsidiaries meet all their responsibilities as set out in this document with regard to the monitoring and remediation of the SHUSA Risk Appetite metrics.

In addition SHUSA expects its subsidiaries to develop their own Risk Appetite monitoring and escalation procedures aligned to SHUSA's.

1.3 Document Ownership and Maintenance

As owner, the Chief Risk Officer ("CRO") is responsible for the development and maintenance of this document. The Enterprise Risk Management function, through its specialist Risk Appetite ("RA") team, has primary responsibility for ensuring the procedures contained herein are implemented on a day to day basis. Due to the relevance of RA reporting the SHUSA Board, this procedure document is approved by the SHUSA Enterprise Risk Management Committee ("ERMC"). It will be reviewed at least annually to ensure that the procedures hereby defined remain relevant to the monitoring of the RAS and the escalation and remediation of metric breaches. The effective date for this document shall be upon approval by the ERMC and implementation is expected to be complete within the following reporting period.

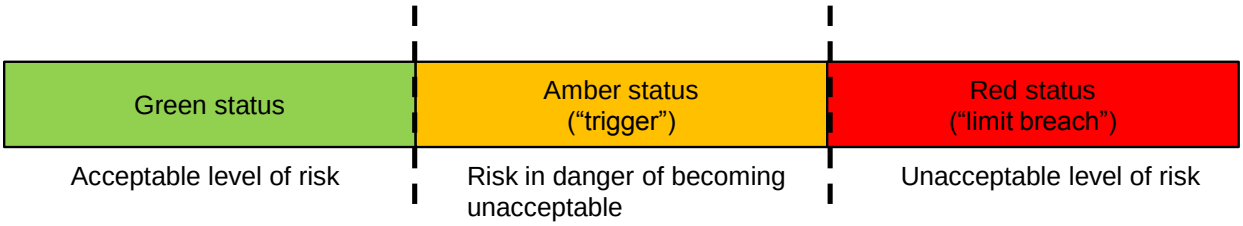
[1] The SHUSA Risk Appetite Metrics Glossary includes the frequency of reporting for each metric, the ownership of the metric and the method of calculation.

2. Risk Appetite Metrics Monitoring and Reporting Process

2.1 Metric Status Definition and Resulting Action

Metrics are assigned one of three status categories – green, amber, or red – based on performance against risk appetite triggers and limits.

Exhibit 1: Metric status definitions



Metrics with green status are within a range that SHUSA is willing to accept. Amber and red statuses, classified as "triggers" and "limit breaches" respectively, indicate that the risk level is in danger of exceeding (amber) or has exceeded (red) the amount of risk acceptable to SHUSA. Both triggers and limit breaches prompt an escalation and remediation process within SHUSA and its subsidiaries.

2.2 SHUSA, Santander S.A and SHUSA Subsidiary Metrics

Risk appetite metrics are approved at both the SHUSA level and at the Subsidiary level. In addition, certain SHUSA RAS metrics are included in the Santander S.A. consolidated Risk Appetite Statement. When they occur, triggers and limit breaches may affect metrics at the Santander Group level, or at SHUSA (e.g., a Subsidiary level metric that is included in the SHUSA RAS or that affects a SHUSA RAS consolidated metric) or only at the Subsidiary level (e.g., certain reputational metrics only applicable at SBNA).

Except where specifically assigned to SHUSA, all roles and responsibilities and actions defined in this procedure document will apply equally at SHUSA and its Subsidiaries.

2.3 Metric Monitoring

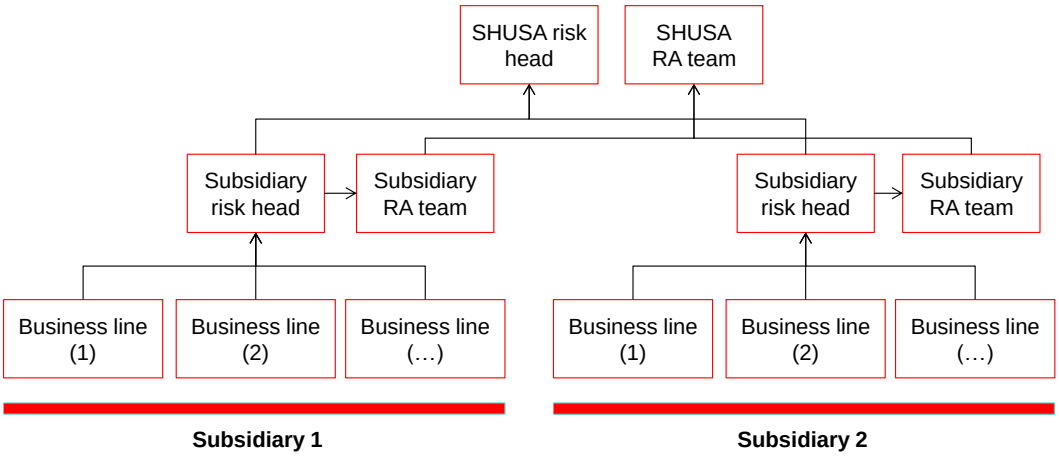
All SHUSA RAS metrics are monitored regularly by the SHUSA Risk Management team working with the Subsidiary Risk Management teams.

The business lines provide data to Risk Managers and RA teams in each Subsidiary on a monthly basis where applicable[2]. SHUSA Risk Managers will work with the Subsidiary teams to aggregate and interpret

[2] Metrics based on the results of the Comprehensive Capital Analysis and Review ("CCAR") such as, for example, CCAR loss budgets, and PPNR impairment, are calculated annually to coincide with the CCAR

the metrics. The Subsidiary RA teams will provide all necessary information to the SHUSA RA team who will be responsible for coordinating the monthly review and aggregation of all SHUSA RAS metrics.

Exhibit 2: Illustrative view of metric monitoring



2.4 Metric Reporting

Once the SHUSA RA team has obtained all risk appetite metric data, it conducts metric analyses, evaluating historical trends and the current status of each metric. The SHUSA RA team produces a report on each metric with the assistance of the risk type owners and Subsidiary RA teams, as well as a summary dashboard that aggregates the output of the analysis. The summary dashboard is sent to the ERMC, the Board Risk Committee ("RC"), and the Board every month for review. All metrics reporting is included in the monthly risk report that is submitted to ERMC. The head of the SHUSA RA team is responsible for submitting information on metrics values and trends to the RC every quarter. Additional presentations are made to the Board at the discretion of the RC.

Metrics at the Subsidiary level are reviewed and reported within the subsidiaries in a process that mirrors that of the SHUSA level metrics at SHUSA.

2.5 Data Validation

Risk Managers are responsible for the accuracy of the data, explanations, and metrics reported. The RA team requests the metric owners to provide supporting documentation each month. In addition, the RA team performs a secondary/backup control to review selected metrics. Every month the RA team selects 1 untested SHUSA RAS metric category (e.g. capital, market risk, etc) and validates back to source documents. This ensures that each RAS category is validated once every six months and twice per

cycle. Furthermore, these metrics are used to derive values for business as usual metrics (e.g., net charge-off rates) that are tracked with a monthly or quarterly frequency.

calendar year. The RA team reviews the metrics and verifies the sampled items agree to source documentation (capital calculations, liquidity, etc.). If any discrepancies are discovered between the source documentation and supplied metric values, there will be further discussion with metric owners to ensure the accuracy of the reported metrics.

The SHUSA RA team will be informed by the Subsidiary RA teams of any discrepancies found by them in the periodic testing of Subsidiary RAS metrics included in the SHUSA RAS and of the actions taken to remediate the discrepancy.

2.6 Recasting Historical Information

In some cases, historical metrics must be recast due to changes in the source data, calculation revisions, changes in methodology, etc. When a need for re-casting is identified, the information is researched with the metric owners and the owner of the source data. Upon conclusion of the research, the metrics are re-casted to reflect the updated information and an explanation to address the reason for the revised data. The SHUSA RA team maintains both the original and the re-casted information in the working master spreadsheet historical files for the SHUSA only metrics.

The Subsidiary RA teams are responsible for maintaining their historical and re-casted data, and to inform the SHUSA RA team of the reasons behind the re-casting.

Re-casted numbers are footnoted in the RAS report to alert the users of the revised numbers.

2.7 Reporting to Santander S.A.

On a quarterly basis the SHUSA RA team produces a report, in the Santander Group approved template, that records the value of Group metrics that are included in the SHUSA RAS. This report is sent to the Santander Group global RA team for monitoring and consolidated Group reporting.

On a monthly basis, a report detailing breaches and including the remediation action plan is sent to the Santander Group RA team for control and monitoring purposes[3].

[3] The reporting to Santander S.A. is described in the "Group Risk Appetite Metrics Collection and Reporting Process"

3. Risk Appetite Metrics Breach Escalation and Remediation Process

3.1 Summary of Escalation Process

In the event that a metric trigger or breach is identified, either through the regular monthly monitoring and reporting cycle or as the result of the first line of defense identifying a breach through its regular business line reporting, the escalation and remediation processes described below must be followed at SHUSA and its Subsidiaries. The goal of escalation and remediation is to ensure (i) the necessary individuals and the entity's governing bodies are notified of a trigger or limit breach and (ii) the appropriate action plan is in place to address the trigger or limit breach. The below procedures are specified to ensure that all necessary parties are notified, and that escalation timelines, responsibilities, and documentation procedures are met.

The escalation path at SHUSA is the primary mode of review and approval of action plans. Most escalation paths, ultimately determined by the SHUSA CRO, are a variation of a standard escalation path, illustrated in the below diagram and described in the remainder of this section.

Exhibit 3: Standard escalation path

3.2 Determination of Appropriate Escalation Path

As a part of ongoing monitoring and reporting, metrics with an amber or red status are flagged by metric owners in collaboration with risk heads and the RA team. The Entity CRO and the SHUSA CRO must be notified immediately after the identification of a trigger or limit breach. Escalation to the CROs must be submitted in writing to ensure that the notification is traceable, but the notification may also be communicated verbally. In the event of a breach of a SHUSA RAS metric included in the Santander S.A. consolidated Risk Appetite Statement the SHUSA CRO is responsible for escalating to the Santander S.A. CRO.

Metric owners and Risk Managers must convene to discuss the trigger or limit breach's cause, severity, impact on the Subsidiary or SHUSA including any potential impact on CCAR based metrics (i.e. risk of breaching total loss budget under stress due to increased Net Charge-Offs), and escalation recommendations.

Following an initial discussion, the metric owners and Risk Managers notify the CROs of their findings.

The SHUSA CRO is ultimately responsible for ensuring that the assigned level and speed of escalation at SHUSA and the Subsidiaries are appropriate based on the potential impact of the trigger or breach on

the enterprise. The SHUSA CRO, in consultation with the Subsidiary CROs, will determine whether and how the escalation process should be expedited, and what additional individuals from risk or the business lines should be included in discussions. For instance, when considering the severity and/or frequency of the breach and the potential impact to the enterprise, the CRO may elect to (i) notify additional individuals of the trigger or limit breach, (ii) expedite escalation to committees, (iii) bypass committees in favor of a direct presentation to the RC or the Board, or (iv) approve stop-gap measures.

In addition to the escalation actions described above the SHUSA CRO in consultation with the Subsidiary CRO will determine (i) whether a trigger or a breach needs to be informed to Internal Audit and / or to the relevant regulators and (ii) who will be responsible for such notification.

3.3 Action Plan Creation and Approval Process

Metric owners are accountable for reporting breaches in accordance with this procedure and for ultimately resolving breaches in the manner approved by the RC or Board. The owners, with the assistance of the risk type head, develop and present a report to the ERMC during the first ERMC meeting scheduled to occur after the trigger or breach has been identified. In cases in which the scheduled ERMC meeting occurs before the metric owners and Risk Managers are able to finalize a proposal for approval, the information available is presented and a subsequent session with the ERMC is scheduled. Certain policies (e.g., Liquidity Policy, Capital Policy) include prescriptive escalation timelines that must be adhered to.

In their report to the ERMC, the metric owners, assisted by the risk type head, are required to provide both an explanation of the trigger or breach and an action plan proposal to remediate the issue. The trigger or breach description and action plan presentations must include:

Trigger / limit breach description	Action plan
• Identification date • An explanation of the metric status and when the status first reached amber and/or red • Historical trend analysis for the metric (preferably no less than one year)	• Description of actions to be taken to remediate trigger/breach • Owner(s) of action plan implementation • Timeline for plan implementation, including timeframe for key milestones • Recommended review plan for ERMC, RC, and Board • Resources required to implement plan

The ERMC reviews the report and refines and approves the action plan.

When a metric is in limit (red) breach, or at the recommendation of the CRO, the metric owners and risk type head additionally present the revised report to the RC. The presentation is slated to occur during the first RC meeting following the ERMC meeting, but the CRO may choose to recommend an earlier

meeting or notify the RC by email. During the meeting, the revised report and action plan are presented, and the RC recommends adjustments and grants approval.

In most instances in which the RC reviews the action plan, the RC is the final body of approval necessary before implementation. The Board is notified of all action plans, but it is only required to approve plans for a trigger or breach if it meets one or both of the following criteria:

- The CRO, with the sign-off of the RC, determines that the trigger or breach is severe enough to warrant Board approval
- The proposed remediation plan involves either adjustment of a RAS metric calibration or a temporary acceptance of a breach of a trigger or limit

In cases in which the Board is required to meet, the presentation is scheduled to occur during the next Board meeting. At the discretion of the CRO and the RC chair, an earlier Board meeting may be scheduled for review and final approval.

For SHUSA metrics included in the Santander S.A. consolidated Risk Appetite Statement the SHUSA CRO, assisted by the SHUSA RA team and the global Risk Appetite function, will be responsible for submitting the action plan for group validation.

3.4 Action Plan Options

Metric owners and Risk Managers should recommend the action plan most appropriate for the metric with the trigger or limit breach, external macroeconomic environment, SHUSA's strategic direction, and SHUSA's ability to execute. The table below outlines a few of the types of action plans that SHUSA or one of its subsidiaries might approve for triggers or limit breaches.

Action Plan	Description
Reduce risk	Reduce risk by acting on metric drivers (immediate or longer-term actions)
Transfer risk	Transfer risk to an external party (e.g., to an insurance company)
Improve operating environment	Indirectly reduce risk by developing or strengthening existing processes; improvements entail gap assessments and resource deployment
Accept risk exceptions	Accept risk in a temporary or one-off exemption; requires Board approval
Adjust appetite limit	Adjust risk appetite for frequently exempted issues to align with evolving business strategies or permanent market changes; requires Board approval

3.5 Action Plan Execution and Monitoring

Once the action plan is approved, the risk type head coordinates the metric owners to ensure that the action steps are carried out. Action plan progress is continually monitored against the designated timeline, and reporting is conducted as recommended. The RA team tracks all triggers and breaches to ensure that action plans are carried out as scheduled.

If milestones are not met within the approved time periods, metric owners again escalate the issue. The metric owners and risk type head notifying Subsidiary leadership and the SHUSA ERMC, RC, and Board of missed deadlines in accordance with the procedure that is specified in the action plan. All changes to implementation timelines must be approved by the highest body that had initially accepted the action plan.

Amber and red metrics are closely monitored and evaluated by all relevant parties until they return to green status. Once green status is attained, the RA team and the risk type head continue to track the metric through the standard monitoring and reporting process to prevent the issue from reoccurring.

3.6 Subsidiary Escalation and Remediation Process – for Subsidiary Only Metrics

The escalation process for Subsidiary only triggers and breaches mirrors that of SHUSA, but occurs at the Subsidiary level. The SHUSA Risk Managers and CRO are also notified, however, they serve in an advisory role to their Subsidiary level counterparts. Similarly, while the SHUSA ERMC retains the right to review and recommend changes to Subsidiary action plans, the Subsidiary ERMC and RC are the parties responsible for action plan review, revision, and final approval.

4. SHUSA Roles and Responsibilities

4.1 Accountability for reporting, monitoring and remediation of triggers and breaches

Risk Appetite management and compliance with triggers and limits will be fostered through the appropriate setting of risk objectives for all SHUSA and Subsidiary staff. Triggers or limit breaches that are not remediated or that frequently reoccur may result in appropriate action being taken with regard to disciplinary action and/or remuneration.

4.2 Overview of Roles and Responsibilities

SHUSA applies three lines of defense principles for managing, monitoring, and mitigating risk. Each line of defense, in SHUSA and the subsidiaries, is engaged in metric monitoring and reporting.

- **Metric owners** – business line, Subsidiary or SHUSA leadership assigned responsibility for a metric by the risk type head or the CRO[4]
- **Risk appetite team (RA team)** – second line of defense team dedicated to risk appetite metric monitoring, evaluation and reporting to the ERMC and the RC;
- **Risk Managers** – second line of defense leadership responsible for monitoring and assessing, as well as providing coordination and support for escalation and remediation of assigned metrics;
- **Audit** – third line of defense team responsible for reviewing and challenging, as necessary, all monitoring, reporting, escalation, and remediation processes

[4] For those metrics where there is a defined relationship between the metric and a business line (e.g., the SBNA Retail portfolio, SHUSA consolidated liquidity metrics), identified metric owners are the heads of the business line. Where a metric applies across multiple business lines, metric ownership is assigned to business line leadership at either SHUSA or at the Subsidiary. Where there is no clear metric owner in the business line, the SHUSA CRO has the authority to select an owner or request that the risk type head fill role requirements.

4.3 Roles and Responsibilities for SHUSA Monitoring and Reporting

The table below describes the roles and responsibilities in the monitoring and reporting process:

Role	Monitoring and reporting responsibilities
First line of defense	
Metric owners	• Regular monitoring of RAS metrics during day-to-day business activities
Second line of defense	
RA team	• Collect current and historical data for each metric • Report and track metrics nearing limits • Develop monthly metric reports and dashboard summaries
Risk Managers	• Review analysis and summary dashboards provided by RA team • Present metric status during normal monitoring and reporting process to ERMC (monthly) and the RC (quarterly)
ERMC	• Evaluate deep-dive analysis presented by metric owners and Risk Managers • Review monthly summary dashboard to track changes in metric status
Third line of defense	
Audit	• Review metric monitoring and reporting process
Outside of three lines of defense	
RC	• Evaluate analysis presented by metric owners and Risk Managers quarterly • Review monthly summary dashboard to track changes in metric status
Board	• Evaluate risk status analysis shared by the RC • Review monthly summary dashboard to track changes in metric status

4.4 Roles and Responsibilities for SHUSA Escalation and Remediation

The table below describes the roles and responsibilities in the escalation and remediation process:

Role	Escalation and remediation responsibilities
First line of defense	
Metric owners	• Immediately inform Risk Managers of trigger or breach • Report triggers and breaches, alongside Risk Managers, to SHUSA and Subsidiary CROs • Develop deep-dive reports to identify issue root causes and create action plans • Present analysis and action plans to ERMC and RC • Oversee implementation of action plans in relevant business lines, re-escalating action plans that do not meet progress milestones
Second line of defense	
RA team	• Provide support to Risk Managers for metric trigger and breach evaluation • Ensure triggers and breaches are escalated according to protocol • Track action plan progress against approved milestones
Risk Managers	• Communicate with CROs, metric owners, and RA teams about triggers and breaches • Notify Subsidiary leadership of SHUSA level issues and remediation plans • Coordinate dialogue with the CROs and metric owners to ensure escalation follows immediately after identification • Facilitate and support metric owners as they develop action plans and present reports
CRO	• Interface with metric owners and Risk Managers to discuss issue root causes • Determine whether escalation should be expedited and notify RC chair and CEO where appropriate • Approve limited subset of emergency actions to adjust 1st LOB activities • Provide input as part of the ERMC on action plans and deep-dive analysis • Notify Subsidiary leadership of SHUSA level issues and remediation plans
ERMC	• SHUSA metrics: refine and approve action plans and timeline proposals, review action plan progress to ensure proper implementation • Subsidiary only metrics: review action plans to ensure alignment with RAS, recommending adjustments where applicable
Third line of defense	
Audit	• Review escalation and remediation process • Review adjustments to RAS calibration
Outside of three lines of defense	

Role	Escalation and remediation responsibilities
RC	• Engage with CRO to provide input and recommendations for the escalation path • SHUSA metrics: refine and approve or review action plans and timeline proposals, review action plan progress to ensure proper implementation • Subsidiary only metrics: review action plans to ensure alignment with RAS, recommending adjustments where applicable
Board	• Review and approve action plans escalated by RC • Approve all temporary exceptions or changes to RAS calibration

5. Document History and Version Control

5.1 Ownership and Authorship

Version	Date	Author	Owner	Change
1.0	October 2015	Risk Appetite Function	Chief Risk Officer	First monitoring, reporting and escalation procedure.

5.2 Sign-Off

Approving Body	Governance Committee Approval or Endorsement	Final Approval Date
Executive Risk Management Committee	Risk Appetite Team	November 17, 2015