Santander Holdings USA, Inc.

BUSINESS CONTINUITY AND DISASTER RECOVERY POLICY

Operating Policy

November 17, 2015

Santander Holdings USA, Inc. ("SHUSA") believes that our success is grounded in our Values, which are also shared by Banco Santander, S.A. and its subsidiaries (collectively with SHUSA, "Santander"). Santander's commitment to treat customers, colleagues and stakeholders in a manner that is *Simple, Personal and Fair* means that every action undertaken by a SHUSA Team Member is founded on *INTEGRITY, CUSTOMER COMMITMENT, PEOPLE, TEAMWORK, OWNERSHIP,* and *INNOVATION*. It is because of this commitment throughout the Santander organization that Santander's customers, clients, and shareholders trust us to deliver world class products and services and select Santander. Safeguarding this trust – by always conducting business responsibly, with integrity and a disciplined approach to risk management – is a responsibility shared by each SHUSA Team Member.

Table of Contents

1. Introduction

1.1 Purpose of the Document

The purpose of the Santander Holdings USA ('SHUSA") Business Continuity and Disaster Recovery Policy ("Policy") is to provide the requirements for developing and maintaining a comprehensive Business Continuity Management Program ("BCMP") across the Enterprise. This Policy will drive resiliency and accountability for all operating units, compliance to regulatory requirements, and the prioritization of business processes and critical operations (including supporting technology) that are essential for recovery.

Unexpected or unplanned disruptions to business operations or technology services may adversely impact SHUSA, its Subsidiaries and customers. Business Continuity and Disaster Recovery ("BC/DR") planning prepares SHUSA, its Subsidiaries, and Third Party Service Providers ("TPSPs"), along with a corresponding technology and telecommunications infrastructure, for a potential disruption of services, emergency, or other disaster. The goal of BC/DR planning is to minimize financial losses to SHUSA and its Subsidiaries and to manage and control risks associated with a disruption of business operations.

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"). This Policy applies to life-safety, facility, technology and telecommunication infrastructure, including information systems, applications, systems, platforms, and computer operations employed in the normal operation of SHUSA, its Subsidiaries and TPSPs. Policies developed by the Subsidiaries must comply with the requirements and standards set forth in this Policy. This Policy will ensure that SHUSA and its Subsidiaries identify, assess, prioritize, manage, and control risk as part of the BCMP process.

1.3 Document Approval and Maintenance

The SHUSA Chief Operational Risk Officer ("SHUSA 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. The Policy is reviewed and approved by the SHUSA Enterprise Risk Management Committee ("SHUSA ERMC") and is approved on an annual basis.

SHUSA Head of Business Continuity Management ("SHUSA Head of BCM") reviews and, if necessary, updates this Policy annually, or when changes occur, to ensure the Policy aligns to regulatory requirements and SHUSA's strategy, current and planned activities. Ad-hoc reviews and updates may be made to this Policy at the discretion of the SHUSA Chief Risk Officer ("SHUSA CRO") and SHUSA ERMC over time based on changes in potential threats, business operations, audit recommendations, and testing results. Changes or updates to the Policy must be developed in consultation with the SHUSA CORO. All material changes must be approved by the SHUSA ERMC.

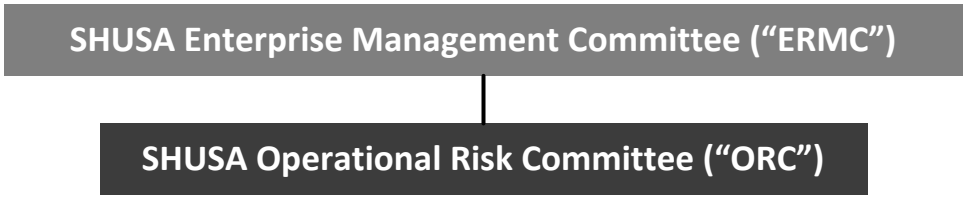
2. Governance and Accountability

2.1 SHUSA Governance

This document is a consolidated Policy for SHUSA and its Subsidiaries. All Subsidiaries must, with respect to Business Continuity Management, adopt and implement the principles set forth in this Policy.

2.2 Policy Governance

This Policy is governed by the following committee structure:



The full responsibilities of the SHUSA ERMC are detailed in its bylaws and committee charters. With respect to this Policy, the SHUSA ERMC 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 ORC recommends this Policy to the SHUSA ERMC for approval on an annual basis or on a frequency as otherwise mandated by the Policy.

The SHUSA ORC reviews this Policy, updates it as necessary, provides input regarding significant changes in accordance with the requirements set forth in Enterprise Risk Management governance, and ensures consistency across SHUSA and its Subsidiaries.

3. Policy

3.1 Policy Statement

It is SHUSA policy to maintain and support a formal contingency planning process to minimize customer impact and risks to the organization in the event of an emergency, disaster, or major unplanned disruption of normal business activity or technology services; including but not limited to a cyber-security incident, pandemic outbreak, and loss of third-party support.

This Policy must be adhered to by SHUSA and its Subsidiaries.

3.2 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 ("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 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.

  SHUSA Subsidiaries are responsible for executing a Business Impact Analyses ("BIA"), BC/DR planning, incident management, regular testing, maintenance, and ensuring compliance within their respective lines of business and corporate functions.

- **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.

  SHUSA and Subsidiary BCMP is part of SHUSA's independent Operational Risk Management ("ORM") function and provides overall oversight, guidance, and direction of the BCMP and processes across SHUSA, its Subsidiaries and TPSPs.

- **Line 2 Legal Function** that is under the executive responsibility of the CEO.

- **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.

Internal Audit conducts independent assessments to ensure compliance with this Policy and related procedures across SHUSA.

3.3 BCMP and Process

SHUSA BCM must establish and document a comprehensive BCMP to support the business line organizational structure for SHUSA and its Subsidiaries and a process to ensure First Line and Second Lines are accountable for BC planning and are ready to execute response and recovery efforts.

SHUSA's business continuity planning process reflects the following components:

1. Continuity Planning Oversight	**2. Business Impact Analysis ("BIA")**	**3. Business Continuity & Disaster Recovery Planning**
4. Business Continuity Management Testing	**5. Incident Management**	**6. Documentation and Reporting**

3.3.1 Continuity Planning Oversight

The SHUSA Board must allocate knowledgeable personnel and sufficient financial resources to properly implement the BCMP and ensure employees are trained and aware of their roles in the implementation and management of the BCMP.

- The SHUSA Head of BCM is responsible for managing and coordinating the SHUSA BCMP and the governance and oversight over the selection, development, and maintenance of SHUSA planning tools and templates for the BIA, risk assessment, BC/DR planning, overall testing, and reporting.
- The SHUSA Head of BCM must ensure that the BCMP is continually updated to reflect the current operating environment and identify required training and awareness to the Subsidiary Head of BCM (2nd LOD).
- Each Subsidiary BCM (2nd LOD) must adopt this Policy or develop a Policy that complies with the requirements and standards set forth in this Policy. The Subsidiary Head of BCM adopt SHUSA Standards or create Standards that support the SHUSA Policy and Standards and must provide documented metrics that support validation of operating within the Policy.
- Where applicable, each SHUSA Subsidiary, under the authority of the SHUSA CORO, must appoint a Subsidiary BCM Team (2nd LOD) to support BC/DR planning and to serve as a Business Continuity Liaison for their unit in the event of an emergency or disaster.
- The Subsidiary Head of BCM must work with the 1st LOD to designate one or more Subsidiary Business Continuity Coordinators ("BCCs") who serve as a liaison between Subsidiary BCM and the business and who organize the execution and maintenance of the BCMP requirements.

- Support the Operational Risk Management policy supporting practices of risk mitigation investment to ensure continuity of operations; ref. Operational Risk Management Policy.

3.3.2 Business Impact Analysis ("BIA")

A BIA is the process of analyzing business processes, identifying their interdependencies, and the effect that a business disruption may have. A Risk Assessment is the identification and evaluation of business continuity risk and mitigating controls for continuity planning and business disruption.

- SHUSA BCM must provide governance and oversight over the selection, development, and maintenance of SHUSA planning tools and templates for the BIA.
- SHUSA BCM must provide oversight and guidance to Subsidiary BCM in completing BIAs, Risk Assessments and will review results of a gap analysis that compares the existing BCMP to the SHUSA Policy and Standards.
- Subsidiary BCM (2nd LOD) must provide oversight and guidance to Subsidiary BCCs (1st LOD) in coordinating and completing the following for new or annual updated BIAs:
    - Completing a BIA for all business processes to determine the criticality and impact to the organization should those operational functions and processes be interrupted,
    - Assigning a criticality rating to each business process to classify the impact a service disruption would have on the line of business, corporate functions, applications, or systems (reference Appendix D – Terms and Definitions – Criticality Rating), and
    - Performing a Risk Assessment to analyze threats that may impact the institution, its customers, and the financial market it serves.
- Subsidiary BCCs (1st LOD) are responsible for the management and execution of a BIA and Risk Assessment for their respective departments or corporate functions.

3.3.3 Business Continuity & Disaster Recovery ("BC/DR") Planning

BC/DR planning ensures the continuity of operations and focuses on the process of developing prior arrangements and procedures that enable SHUSA and its Subsidiaries to:

- Respond to an event in such a manner that critical business processes may continue to operate within planned levels of disruption, and
- Ensure technology continuity readiness and information technology systems that support critical business processes are recoverable in the event of a major system disruption.

- SHUSA BCM must provide oversight, guidance, compliance requirements and measurements to the Subsidiary BCM in developing BC/DR strategies, processes, and procedures.
- Subsidiary BCM (2nd LOD) must provide oversight to the BCCs (1st LOD) and ensure that BC/DR requirements are followed across their entity to maintain a recovery environment with a high level of continuity readiness.
- Subsidiary BCM (2nd LOD) must establish all BC/DR templates developed for the BCMP which will be reviewed by the SHUSA Head of BCM or designee and updated annually to address changes in the organization, business, technology, risks, and external factors.
- Subsidiary BCM (2nd LOD) must provide guidance and oversight to the 1st LOD in developing BC/DR Plans.

- Subsidiary BCCs (1st LOD) are responsible for the management and execution of BC/DR planning for their respective departments or corporate functions and perform scheduled testing using an

integrated methodology at the site level or at a minimum with other application dependencies and/or third party providers that support a business process.

3.3.4 Business Continuity Management Testing

- SHUSA BCM must provide governance and oversight to the Subsidiaries in the development of business continuity testing strategy and test plans that incorporate the use of the BIA, recovery planning strategies, and the involvement of staff, technology, facilities, internal and external business process dependencies and third party service providers.
- Subsidiary BCM (2nd LOD) must provide oversight and guidance to the BCCs in conducting testing for their respective departments, corporate functions, technology, and third-party providers.
- Subsidiary BCCs (1st LOD) are responsible for the management and execution of testing with the focus on recovery time objectives and recovery strategies assigned to each business process and test scenario, document test results, and ensure sufficiency to meet continuity objectives.

3.3.5 Incident Management

Incident management focuses on instituting comprehensive plans of action for responding to a disruptive or potentially disruptive incident, and manages the activation and coordination of plans at the time of disruption.

- SHUSA BCM must provide guidance and oversight to each Subsidiary's BCM in the development of an Incident Management Plan ("IMP") which incorporates an Incident Management Team ("IMT") and outlines procedures for the declaration of a disaster event or incident.
- Subsidiary BCM (2nd LOD) must develop and maintain an individual IMP and IMT to support their organization.
- Where applicable and resulting from an incident, SHUSA Subsidiary BCM must conduct a "Post-Mortem" meeting with participants from Subsidiaries' IMT and the 1st LOD, to discuss incidents, their root cause(s) and effect(s), short term and long term remediation plans, and must report findings to the SHUSA Head of BCM for review who in-turn will report to the SHUSA ORC.

3.3.6 Documentation and Reporting

- SHUSA BCM must report the status of the SHUSA and Subsidiary BCMPs on an annual basis and report to the Subsidiary Governance, SHUSA CORO, SHUSA CRO, SHUSA ERMC, and the SHUSA Board annually, or as required.
- Subsidiary BCM must provide documentation, reporting, testing results, and metrics to SHUSA Head of BCM annually, or as required.
- Subsidiary BCC (1st LOD) must establish and maintain BC/DR Plans to ensure that critical operations and business processes (Reference Criticality Ratings in Appendix 8.4) are operational in the event of a disaster or service disruption.

3.4 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 Business Continuity project plan.

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

3.5 Policy Enforcement

This Policy is enforced by the SHUSA Board with 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 access to computer and/or network resources;
- Suspension or termination of employment, to the extent authorized by other published policies and procedures; and/or
- Suspension or termination of contract computer and/or network services.

4. Roles and Responsibilities

4.1 Subsidiary Heads of Business Continuity Management ("Subsidiary Heads of BCM")

As part of the 2nd LOD, the Heads of BCM for SHUSA Subsidiaries own the BCMP for their organization. Duties include coordinating, maintaining, and performing regular review and testing of BIAs and BC/DR Plans. These teams and/or individuals are responsible for the governance of an effective BCMP, ensuring application and adherence to this Policy and the Subsidiary policy, and keeping the Subsidiary BCMP up-to-date to reflect the current operating environment.

4.2 Subsidiary Business Continuity Coordinators ("Subsidiary BCCs")

As part of the 1st LOD, BCCs are appointed by their Lines of Business to serve as a liaison between the Subsidiary BCM and the business. BCCs coordinate, complete, maintain, and perform regular review and testing of their BIA(s) and BC/DR Plan(s). These individuals are responsible for management and execution of an effective BCMP, ensuring application and adherence to this Policy and keeping their BIA(s) and BC/DR Plan(s) up-to-date to reflect their current operating environment.

4.3 Subsidiary Operational Risk Management ("Subsidiary ORM")

As part of the 2nd LOD, the Subsidiary BCM organization is directly accountable to the SHUSA Head of BCM for the governance, oversight, and training of BC/DR Policies and Standards and for operating in accordance with it. This includes, where applicable, reporting and event escalations from the Subsidiary operational risk officers to the SHUSA Head of BCM.

4.4 SHUSA Chief Operational Risk Officer ("SHUSA CORO")

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 has delegated certain administrative responsibilities for this Policy to the SHUSA Head of BCM. Additionally, the SHUSA CORO is responsible for approving results of BIA and BC/DR reporting to the SHUSA ERMC.

4.5 SHUSA Head of Business Continuity Management ("SHUSA Head of BCM")

As part of the 2nd LOD, the SHUSA Head of BCM is responsible for maintaining this Policy and for managing and tracking exceptions to this Policy. The SHUSA Head of BCM is responsible for developing all BCM elements across all of SHUSA.

4.6 Internal Audit

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

4.7 SHUSA Board of Directors ("SHUSA Board")

The SHUSA Board must ensure that this Policy is followed by all lines of business and corporate functions across SHUSA. The SHUSA Board must ensure necessary resources and funding are allocated to support the Policy.

4.8 SHUSA Risk Committee ("SHUSA RC")

The SHUSA RC 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 RC reviews and approves the BCMP and recommends to the SHUSA Board key 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, including the review of BC/DR processes and procedures, as necessary.

4.9 SHUSA Enterprise Risk Management Committee ("SHUSA ERMC")

The SHUSA ERMC is responsible for overseeing the development, implementation and maintenance of the SHUSA's BCMP and is established under the authority of the SHUSA RC and is chaired by the SHUSA CRO. SHUSA ERMC is responsible for the oversight and monitoring of all risk-taking and risk management activities across the enterprise. The SHUSA ERMC reviews the BCMP for approval of the SHUSA BCMP on an annual basis or on a frequency as otherwise mandated by this Policy.

4.10 SHUSA Operational Risk Committee ("SHUSA ORC")

The SHUSA ERMC and CRO established the SHUSA ORC to oversee operational risk. SHUSA ORC has the primary responsibility to oversee and manage the identification and monitoring of operational risk in SHUSA and its Subsidiaries. The SHUSA ORC through the SHUSA CORO advises the SHUSA ERMC and Subsidiary governance committees on the supervision, control and reporting of the BCM operational risks related to Subsidiary operations and activities. The ORC oversees adherence to the Policy across the enterprise regarding BCM operational risk and recommendations from internal audit, external audit, and regulators with regard to the BCMP.

4.11 SHUSA Chief Risk Officer ("CRO")

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

4.12 Human Resources ("HR")

HR is engaged during the Policy infraction process and when input is required on the appropriate decision for Policy violations

4.13 Learning & Development ("L&D")

Santander L&D provides SHUSA and its Subsidiaries access to tools and resources that enable team members to pursue functional knowledge, professional and leadership development needed to grow team members' skills, and mitigate risk to their respective business units.

SHUSA BCM will work with the Subsidiary BCM to identify training needs and communicate to the SHUSA Head of BCM and Subsidiary Head of BCM (2nd LOD). The Subsidiary 2nd LOD will develop, deliver and provide ongoing BCM training and awareness to the Subsidiary 1st LOD.

5. Reporting Structure

The SHUSA Head of BCM provides oversight, ensures effective controls are in place, and implements an integrated enterprise-wide Policy and Standards through coordination with the operational risk leads within SHUSA and each Subsidiary. The SHUSA Head of BCM reviews and reports on the status of Subsidiary critical BIAs and BC/DR Plans to the SHUSA CORO on an annual basis or as required. The SHUSA Head of BCM monitors, reviews and approves the metrics results, event reports including but not limited to post-mortem reports and activities, and reports and / or escalates the status to the SHUSA CORO.

The SHUSA CORO monitors, reviews, and approves the results of the BIA and risk assessment. The SHUSA CORO also reports on the status of the SHUSA BCMP to the SHUSA ERMC on an annual basis.

6. 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 Head of BCM and will be included in the annual report to the SHUSA ERMC.

7. Document History and Version Control

7.1 Ownership and Authorship

Version	*Date*	*Author*	*Owner*	*Change*
1.0	*February 6, 2014*	*SHUSA Head of BCM*	*SHUSA CORO*	*Initial Version*
2.0	*May 5, 2015*	*SHUSA Head of BCM*	*SHUSA CORO*	*Enhancement for Enterprise Policy Administration Policy*
3.0	*November 17, 2015*	*SHUSA Head of BCM*	*SHUSA CORO*	*Enhancements to the BC/DR Policy*

7.2 Sign Off

Approving Body	*Governance Committee Endorsement*	*Date*
SHUSA Operational Risk Committee ("ORC")	*SHUSA ORC*	October 8, 2015
SHUSA Enterprise Risk Management Committee ("ERMC")	*SHUSA ERMC*	November 17, 2015

8. Appendices

8.1 Appendix A – Key Contacts

Title	*Role*	*Name and Contact*
Chief Operational Risk Officer	*Policy Owner*	*Michael Lima, SVP, SHUSA Interim Chief Operational Risk Officer mlima1@santander.us*
Head of Business Continuity Management	*Primary point of contact on Policy related matters*	*Danny Phillips, SVP, Business Continuity Management Director danny.phillips@santander.us*

8.2 Appendix B – Regulatory Obligations Addressed by this Policy

Regulatory Agency	*Citation*	*Title*
FFIEC	*http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning.aspx*	*Business Continuity Planning BCP February 2015*

8.3 Appendix C – Related Policies and Process and Administrative Documents

Document Type	*Entity and Department*	*Owner*	*Document Title*
Policy	*SHUSA Operational Risk - TPRM*	*Chief Operational Risk Officer*	*SHUSA Enterprise Third Party Risk Management Policy*
Framework	*SHUSA Operational Risk – Operational Risk Management*	*Chief Operational Risk Officer*	*SHUSA-Operational Risk Management Framework*
Policy	SHUSA Operational Risk – Operational Risk Management	*Chief Operational Risk Officer*	*SHUSA Operational Risk Management Policy*
Standards	SHUSA Operational Risk - BCM	*Chief Operational Risk Officer*	*SHUSA-Business Continuity Management Standards (In Progress)*

8.4 Appendix D – Terms and Definitions

Business Continuity Management Program ("BCMP")

An ongoing management and governance process supported and resourced by lines of business and corporate function heads to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure continuity of products/services through testing, training, maintenance, and assurance.

Business Continuity Plan ("BC Plan")

A formal, written contingency plan that documents the steps necessary to ensure that a line of business and corporate function can recover from service interruption due to a disaster or emergency. It includes information such as criticality rating, site and human resource information, business recovery strategy, major function and system descriptions, vital records and documents, impact of losses, emergency team information, resource needs, and testing frequency.

Business Continuity Test Plan ("BC Test Plan")

A formal procedural document that guides testing of the BC Plan. It includes information such as testing frequency, testing procedures and test results.

Business Impact Analysis ("BIA")

Predicts the consequences of disruption of a business function and process and gathers information needed to develop recovery strategies. Potential loss scenarios are identified during a Risk Assessment, i.e., operations may be interrupted by the failure of a supplier of goods or services or delayed deliveries.

Criticality Rating

Operational loss events and control failures result in the loss of facilities, people, systems, internal business process dependencies, or third party vendors. A five-tiered measurement classifies the impact a service disruption would have on lines of business, corporate functions, applications, or systems. The impact categories measured against the rating scale are defined as financial, legal, regulatory, contractual, customer, reputation, and business operations. The criticality ratings are:

- High - significant adverse impact to the business: Recovery Time Objective – 0 to 8 hours.
- Elevated - relatively large adverse impact to the business: Recovery Time Objective – 8 to 24 hours.

- Moderate - some marginal adverse impact to the business: Recovery Time Objective – 24 to 72 hours.
- Moderate–Low - limited adverse impact to the business: Recovery Time Objective - 3 to 10 days.
- Low - negligible or no adverse impact to the business: Recovery Time Objective – 10 days+.

Disaster Recovery Plan ("DR Plan")

A formal plan that documents the process of identifying critical computing and telecommunications resources and the potential events that could affect SHUSA's ability to function and to restore business operations. It provides detailed procedures for emergency response and extended back-up operations, as well as post-technology DR activities for SHUSA's computer and telecommunications operations, infrastructure, and testing frequency.

Disaster Recovery Test Plan ("DR Test Plan")

A formal procedural document that guides testing of the Technology DR Plan that includes information related to testing procedures, test results, affiliates, and third parties.

Post-Mortem Meeting

A review of what happened throughout the lifecycle of an incident or disaster. A good post-mortem delves into the "who, what, where, how, when, and why" of an incident. Even if the incident was clearly documented at the time, a review is still needed to assess how the event could have been managed better in order to improve processes, tools, and training for the future. These improvements may not prevent all future attacks, but they provide readiness, response, and recovery for the next incident.

Risk

The chance of something happening, which will have a consequence. It is measured in terms of impact and likelihood.

Risk Assessment

The determination of quantitative or qualitative value of risk related to a concrete situation and a recognized threat.

Third Party Service Provider ("TPSP")

A TPSP is an entity or person that has entered into a business relationship with SHUSA or its Subsidiaries to perform or provide one or more of the following activities:

- Products or services directly or indirectly to SHUSA or its Subsidiaries.
- Functions of SHUSA or Subsidiary operations.
- Business on behalf of SHUSA and its Subsidiaries, or refers or sells SHUSA products.
- Products or services directly or indirectly to any current or prospective customer of SHUSA and its Subsidiaries in connection with SHUSA's offer or provision of financial services.