

Santander Holdings USA, Inc.



INFORMATION RISK MANAGEMENT ENTERPRISE POLICY

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	5
1.1 PURPOSE OF THE DOCUMENT	5
1.2 SCOPE	6
1.3 DOCUMENT APPROVAL AND MAINTENANCE	6
1.4 KEY TERMS.....	7
2. GOVERNANCE AND ACCOUNTABILITY	10
2.1 POLICY GOVERNANCE	10
3. POLICY.....	11
3.1 POLICY STATEMENT.....	11
3.2 THREE LINES OF DEFENSE.....	11
3.3 ASSURANCE MANAGEMENT	12
3.3.1 RISK MANAGEMENT.....	12
3.3.2 AUDIT MANAGEMENT	12
3.3.3 COMPLIANCE MANAGEMENT.....	13
3.3.4 BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY MANAGEMENT.....	13
3.3.5 VENDOR MANAGEMENT	14
3.4 IDENTITY AND ACCESS MANAGEMENT	14
3.4.1 ACCESS PROVISIONING AND DE-PROVISIONING	14
3.4.2 ROLE MANAGEMENT.....	15
3.4.3 AUTHENTICATION AND AUTHORIZATION	15
3.4.4 ATTESTATION AND CERTIFICATION	16
3.5 SECURITY AND PRIVACY MANAGEMENT	16
3.5.1 POLICIES AND STANDARDS MANAGEMENT	17
3.5.2 SECURITY ARCHITECTURE AND SECURE BUILDS.....	17
3.5.3 DATA PROTECTION.....	18
3.5.4 PHYSICAL AND ENVIRONMENTAL	18
3.5.5 TRAINING AND AWARENESS	19
3.6 OPERATIONS MANAGEMENT	19
3.6.1 MONITORING	20
3.6.2 BACKUP AND STORAGE	20
3.6.3 NETWORK AND SECURITY OPERATIONS.....	21
3.6.4 PROCESS AUTOMATION.....	21
3.7 CONFIGURATION MANAGEMENT.....	22
3.7.1 INVENTORY AND CONFIGURATION MANAGEMENT.....	22
3.7.2 PATCH MANAGEMENT	23
3.7.3 SOFTWARE DISTRIBUTION.....	23
3.7.4 VIRTUAL MANAGEMENT.....	24
3.8 SERVICE MANAGEMENT	24
3.8.1 ASSET MANAGEMENT.....	24
3.8.2 CHANGE & RELEASE MANAGEMENT.....	25

3.8.3	PROBLEM AND INCIDENT MANAGEMENT.....	25
3.8.4	SYSTEM DEVELOPMENT LIFE CYCLE AND SOFTWARE ACQUISITION.....	26
4.	ROLES AND RESPONSIBILITIES	26
4.1	SHUSA CISO (2 ND LINE):.....	26
4.2	SHUSA DIRECTOR, IT RISK AND SECURITY (1 ST LINE):	27
4.3	SHUSA CIO (1 ST LINE):	27
4.4	SHUSA CHIEF OPERATIONAL RISK OFFICER	27
4.5	INTERNAL AUDIT (3 RD LINE):.....	27
4.6	BOARD OF DIRECTORS	27
4.7	RISK COMMITTEE	27
4.8	ENTERPRISE RISK MANAGEMENT COMMITTEE	28
4.9	SHUSA OPERATIONAL RISK MANAGEMENT COMMITTEE	28
4.10	SHUSA CHIEF RISK OFFICER	28
5.	REPORTING STRUCTURE	28
6.	IMPLEMENTATION, ENFORCEMENT, AND EXCEPTIONS	28
7.	DOCUMENT HISTORY AND VERSION CONTROL	30
7.1	OWNERSHIP AND AUTHORSHIP	30
7.2	SIGN OFF	30
8.	APPENDICES	31
8.1	APPENDIX A – KEY CONTACTS	31
8.2	APPENDIX B – REGULATORY OBLIGATIONS ADDRESSED BY THIS POLICY.....	31
8.3	APPENDIX C – RELATED POLICIES AND PROCESS AND ADMINISTRATIVE DOCUMENTS	32

1. Introduction

1.1 Purpose of the Document

The purpose of the Santander Holdings USA, Inc. (“SHUSA”) Information Risk Management Policy (“Policy”) is to establish enterprise-wide requirements, principles, and highlight regulatory guidelines that apply to information risk management and governance for SHUSA operations and its material operating subsidiaries (“Subsidiaries”). The Policy supports the board of directors (“Board”) and management by documenting established operating parameters within which SHUSA and its Subsidiaries will protect company information. This Policy ensures that SHUSA and its Subsidiaries are committed to safe and sound information risk management practices.

To ensure all information technology (“IT”) and information risk-related regulatory and internal mandates are complied with throughout the organization, SHUSA utilizes a requirements library that harmonizes over 118 authoritative sources and over 4,000 individual mandates. This includes both external (comprised of Federal Financial Institutions Examination Council's (FFIEC) handbooks, Gramm–Leach–Bliley Act (GLBA), Payment Card Industry Data Security Standard (PCI DSS), privacy laws, etc.) and internal mandates. These mandates are mapped to an Information Risk Framework. The SHUSA Information Risk Framework provides the hierarchical structure by which policies and standards are communicated down to organizational units, as well as by which risk is aggregated and reported up to the Board.

The requirements incorporated into the framework are translated into this Policy. As specified by this Policy, SHUSA and its subsidiaries shall develop supporting policies and standards to address details applicable to each risk topic. This Policy addresses all internal and external mandates integrated into the Information Risk Requirements Library. This includes all information security mandates which ensures the Policy meets the requirements of the SHUSA Information Risk Management Program.



Figure 1. SHUSA Risk Management Framework

1.2 Scope

The Policy applies to SHUSA and its Subsidiaries which include Santander Bank, N.A. (“SBNA”) and Santander Consumer USA (“SCUSA”). Operating policies developed by the Subsidiaries must comply with the requirements and standards set forth in this Policy.

Given the heightened sensitivity with respect to Cyber Security, this Policy is designed to be comprehensive of all aspects pertaining to Cyber Security.

This Policy applies to information assets including those in electronic (e.g., information systems, applications, systems platforms and computer operations) and physical (e.g., vendor contracts, loan documentation, credit files, signature cards and personnel information) formats employed in normal operations. This includes information assets processed, transmitted or stored by third party service providers.

1.3 Document Approval and Maintenance

This Policy is owned by the SHUSA Chief Information Security Officer (“CISO”). It is approved by the SHUSA Board. It is reviewed and agreed to by the Board Risk Committee, the SHUSA Enterprise Risk Management Committee (“ERMC”), the SHUSA Operational Risk Management Committee (“ORMC”), the SHUSA Chief Information Officer (“CIO”) and the SHUSA Director of IT Risk and Security.

The Policy:

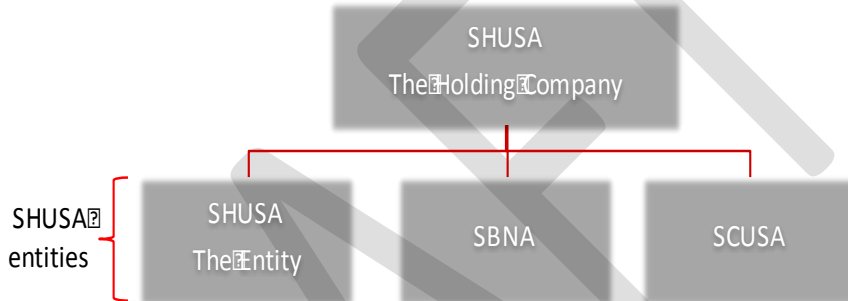
- Is reviewed and approved at least annually to assure it remains relevant to and applicable to SHUSA’s current and planned activities. In addition to scheduled policy reviews, ad-hoc reviews can be initiated by the SHUSA CISO , the SHUSA Director of IT Risk and Security, T&O Governance, Risk and Compliance (“GRC”), the SHUSA CIO, the ERM, the ORM or Board Risk Committee at any time and performed as needed to incorporate updates. Any material updates made to this Policy are approved by the Board.
- Shall be clearly defined and consistent with the nature and complexity of SHUSA’s activities and consider all pertinent laws and regulations. As regulatory changes occur, it is reviewed and updated on a timely basis.
- Shall be communicated to all stakeholders, assuring that the people responsible for its application and fulfillment acknowledge and use them in their day-to-day operations.

1.4 Key Terms

The following definitions are used within this document.

Access	Ability and means to enter a facility, to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions. Adapted from CNSSI 4009
Access control	Limiting access to organizational assets only to authorized entities (e.g., users, programs, processes, or other systems). See asset. Adapted from CNSSI 4009
Access management	Management processes to ensure that access granted to the organization’s assets is commensurate with the risk to critical infrastructure and organizational objectives. See access control and asset. Adapted from CERT RMM
Administrative Account	An account with administrative access (typically for <u>infrastructure</u>).
Application	Software that is designed for an end user in the support one or more business processes. Also referred to as “application software” or “end-user program”. An application can be comprised of Applications, IT Systems, and Components.
Application Certification	The process of reviewing the application details and user access used to conduct the User Entitlement Reviews (UERs).
Audit Management	The capability of performing reasonable and appropriate independent verification and validation of the SHUSA operating environment’s risk management and control capabilities, compliance readiness, and disaster preparedness
Authentication and Authorization	One of the Identity & Access Management Risk Topics. The capability to positively identify a user or system (i.e., authentication) and approve entitlements and/or roles (i.e., authorization) to access targets.
Business Continuity and Disaster Recovery Management	The capability of designing, developing, implementing, and monitoring resiliency safeguards intended to maintain a level of disaster preparedness and availability sufficient to address SHUSA’s requirements
Business impact analysis	A mission impact analysis that prioritizes the impact associated with the compromise of an organization’s information assets, based on a qualitative or quantitative assessment of the sensitivity and criticality of those assets. NIST SP800-30

Business Role Certification	The process of certifying the appropriateness of entitlements and application roles assigned to a business role.
Cardholder Data Environment	Defined by PCI 3.0 as [Cardholder Data Environment (CDE) includes all processes and technology as well as the people that store, process or transmit customer cardholder data or authentication data, including connected system components and any virtualization components (i.e., servers, applications, etc.)"
Configuration management	A collection of activities focused on establishing and maintaining the integrity of assets (i.e., hardware, software, documentation), through control of the processes for initializing, changing, and monitoring the configurations of those assets throughout their life cycle.
Deprovisioning	The process of revoking or removing an identity's access to organizational assets.
Environmental Controls	Measures which provide physical protection of information assets against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disasters.
Identity & Access Management (IAM)	One of the IRM Framework Risk Categories. IAM comprises four risk topics (Provisioning & Deprovisioning, Role Management, Attestation and Certification, and Authentication and Authorization.)
Incident Response Plan	An outline of the steps to be taken when identifying, responding to, reporting, and mitigating security incidents, which is developed, implemented, disseminated and communicated to appropriate SHUSA Workforce Members.
Information assets	Information or data that is of value to the organization, including diverse information such as operational data, intellectual property, customer information, and contracts. CERT RMM
Information Security	Information Security is the processes, policies, and procedures of protecting information systems from unauthorized access, improper use, disclosure, disruption, modification or destruction. GARP-ORM
Inherent Risk	Category of threat that describes potential losses or pitfalls that exist before internal security controls or mitigating factors are implemented.
Issue/Incident Management	The process through which the capability of identifying, analyzing, preventing and remediating problems and incidents is managed.
IT System	Software and data (and possibly the underpinning hardware) that support business processes and/or other support processes, but is not designed for end user interaction. An IT System can be comprised of Applications, IT Systems, and Components. An IT System can support one or more Applications and IT Systems.
Least Privilege	Access is granted with an appropriate business justification and with only the minimum access rights necessary to perform the job function.
Nonpublic personal information	Generally is any information that is not publicly available and that: <ul style="list-style-type: none"> • A consumer provides to a financial institution to obtain a financial product or service from the institution; • Results from a transaction between the consumer and the institution involving a financial product or service; or • A financial institution otherwise obtains about a consumer in connection with providing a financial product or service. GLBA
Provisioning and De-Provisioning	One of Identity & Access Management Risk Topics. The capability of adding (i.e., provisioning), removing (i.e., de-provisioning), or changing accounts, entitlements, and roles for users and systems interacting with access targets.

Separation of Duties (SoD)	[A security control that] "addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions. Organizations with significant personnel limitations may compensate for the separation of duty security control by strengthening the audit, accountability, and personnel security controls". NIST 800-53
User Entitlement Review	Attestation of the entitlements and roles assigned to users (typically workforce members)
SHUSA Entities	<p>The use of the term "SHUSA entities" or "entities" within this document refers collectively to the subsidiary companies of the SHUSA Holding Company as well as to the SHUSA entity itself. The graphic below clarifies this relationship:</p>  <pre> graph TD SHUSA_HC[SHUSA Holding Company] --> SHUSA_Entity[SHUSA The Entity] SHUSA_HC --> SBNA[SBNA] SHUSA_HC --> SCUSA[SCUSA] SHUSA_Entity --- SHUSA_entities_group[SHUSA entities] SBNA --- SHUSA_entities_group SCUSA --- SHUSA_entities_group </pre>
Workforce Members	Employees, contractors, vendors, interns, volunteers, trainees, and other persons whose conduct, in the performance of work for SHUSA, is under the policies, standards, etc. of SHUSA, whether or not their employment is directly with SHUSA.

2. Governance and Accountability

This document is a consolidated Enterprise Policy for SHUSA and its Subsidiaries. All Subsidiaries must, with respect to their Information Risk (and/or Information Security) Management functions, adopt and implement the principles set forth in this Enterprise Policy.

2.1 Policy Governance

This Policy is governed by the following committee structure:



Full SHUSA Board responsibilities 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 for approval to the SHUSA Board.

The SHUSA 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 ORMC 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

The SHUSA Board and senior management have adopted the following policy statements to address internal and external information risk mandates. These policy statements, which will apply to all activities across the enterprise, will be carried out and given more complete effect by other related policies, programs, standards and procedures as may be adopted from time to time in accordance with this Policy.

SHUSA entities shall establish policies and standards in order to effectively implement this enterprise Policy.

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.

Line 1 shall be responsible for identifying, assessing, mitigating, managing operational risk, including information risk, and ensuring compliance within its respective area(s).

- **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.

Operational Risk Management is part of SHUSA’s independent Risk Management function, which includes Information Risk Management, that provides supervision of the operational risk management program and processes across SHUSA and its Subsidiaries.

- **Line 3 (“Third Line of Defense” or “3rd LOD”) Risk Assurance. 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 shall 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 of risk and compliance related procedures across SHUSA, including those concerning information risk.

3.3 Assurance Management

Assurance Management defines the necessary capabilities to provide reasonable verification that controls intended to manage the confidentiality, integrity and availability of information are designed and operating effectively to address risk, compliance, audit and resiliency requirements and objectives. It addresses the establishment of capabilities regarding risk management, audit management, compliance management, business continuity, disaster recovery and vendor management.

Entity 2nd Line risk functions will ensure the following policy statements are implemented via standards:

3.3.1 Risk Management

The capability of identifying information risks, qualitatively and quantitatively assessing information risks, determining information risk treatment, and managing associated findings and remediation plans will be managed with a defined process. Risk Management will be performed for information systems that store, transmit, or process information assets as well as related processes, vendors (i.e., Third-Party Service Providers), facilities, and functions. An organization-wide information risk assessment will be performed at least annually or upon significant changes to the environment (for example, acquisition, merger, relocation, etc.).

Standards shall assign responsible parties for at least the following requirements:

Requirement	Accountable Unit(s)
Conduct self-assessments with business units.	1 st Line
Implement information risk management program for information assets.	2 nd Line

3.3.2 Audit Management

The capability of performing reasonable and appropriate independent verification and validation of the operating environment's risk management and control capabilities, compliance readiness, and disaster preparedness shall be managed with a defined process. The audit management process will cover information systems (e.g., applications, operating systems, network devices) that store, transmit, or process information assets, related processes, vendors (i.e., Third-Party Service Providers), facilities, and functions that are in-scope for compliance related mandates applicable to SHUSA.

These information security audit management requirements are incorporated into the Enterprise Audit Policy. Roles and responsibilities are likewise defined within that document.

3.3.3 Compliance Management

The capability of identifying compliance requirements, assessing compliance readiness, determining potential compliance gaps and recommended treatments, and managing associated findings and remediation plans will be managed with a defined process. Compliance Management will be performed for information systems (e.g., applications, operating systems, network devices) that store, transmit, or process information assets, related processes, vendors (i.e., Third-Party Service Providers), facilities, and functions that are in-scope for compliance related mandates applicable to SHUSA. Compliance readiness ratings will be determined and documented. SHUSA entities shall maintain awareness of compliance requirements and the threat landscape by membership in information sharing entities (e.g., Financial Services – Information Sharing and Analysis Center (FS-ISAC), the CERT Coordination Center, etc.) as well as coordination with local, state and federal government agencies.

Standards shall assign responsible parties for at least the following requirements:

Requirement	Accountable Unit(s)
Implement processes to ensure legal and policy compliance	2 nd Line
Develop and manage a policy and standard exception process in alignment with the risk management methodology	2 nd Line
Establish and maintain contact with Information Security related external bodies	2 nd Line
Identify applicable Information Security legislation	2 nd Line
Support the ongoing analysis of information resources relative to compliance expectations with the second line of defense.	1 st Line

3.3.4 Business Continuity Planning and Disaster Recovery Management

The capability of designing, developing, implementing, and monitoring resiliency safeguards intended to maintain a level of disaster preparedness and availability sufficient to address business requirements will be managed with a defined Business Continuity Process (BCP) and Disaster Recovery (DR) process. Such a process will include the performance of a Business Impact Analysis (“BIA”), and the development of a Disaster Recovery Plan (“DRP”) for information systems that store, transmit or process information assets as well as related processes, vendors (i.e., Third-Party Service Providers), facilities, and functions. Such plans will be documented, tested, reviewed and updated as deemed reasonable and appropriate by entity management. At a minimum, the Board of each entity will annually update and approve the entity’s business continuity plans. Management will also report the tests of the plan and back-up systems to the Board on an annual basis.

These information security requirements are incorporated into the Enterprise Business Continuity and Disaster Recovery Management Policy. Roles and responsibilities are likewise defined within that document.

3.3.5 Vendor Management

Each SHUSA entity identifies and manages risks to information assets managed by third-party service providers through due diligence during the selection process and on-going vendor oversight. Entities will oversee and monitor third-party service providers by directly auditing the service provider's operations and controls, employing the services of external auditors to evaluate the servicer's controls, or receive sufficiently detailed copies of audit reports from the service provider.

These information security requirements are incorporated into the Third Party Risk Management Policy. Roles and responsibilities are likewise defined within that document.

3.4 Identity and Access Management

Identity and Access Management defines the capabilities necessary to ensure effective and risk commensurate information access controls. It addresses the establishment of capabilities regarding provisioning, de-provisioning, role management, authentication, authorization, attestation and certification.

Entity 2nd Line risk functions will ensure the following policy statements are implemented via standards:

3.4.1 Access Provisioning and De-Provisioning

SHUSA entities shall develop provisioning and de-provisioning standards to ensure that:

- Formal approval is obtained and documented prior to granting access.
- Auditable records of provisioning and de-provisioning activities are maintained.
- To the extent possible, access controls enforce the principle that everything is forbidden unless expressly permitted, access is the minimum necessary for business purposes (a.k.a. principle of least privileged), and separation of duties is enforced. These restrictions apply to entitlements and roles for both human users as well as software programs.
- Access is terminated promptly when no longer required.

Standards shall assign responsible parties for at least the following requirements:

Requirement	Accountable Unit(s)
Establishing and maintaining an account management process	1 st Line
Performance of background checks for users needing privileged access	1 st Line
Ensuring that all team members sign confidentiality and non-disclosure agreements	1 st Line

Verification of account entities prior to a password reset	1 st Line
Ensuring entitlements are appropriate as job requirements and the business environment changes	1 st Line
Checking for dormant accounts and either disabling or removing access	1 st Line
Identifying and notifying appropriate parties of terminations and leaves of absence	1 st Line
Ensuring provisioning processes check for separation of duty requirements	1 st Line

3.4.2 Role Management

SHUSA entities shall develop appropriate role management standards to ensure that:

- Roles are managed with a defined process for defining, assigning and maintaining such roles.
- Roles are defined on a 'least privilege' basis and do not violate separation of duty.
- Entitlements associated with roles are documented, reviewed and approved by the Application Owners, Business Owner, and/or Role Owners.

Standards shall assign responsible parties for at least the following requirements:

Requirement	Accountable Unit(s)
Ensure roles are managed with a defined process for defining, assigning and maintaining such roles	1 st Line
Ensure roles are evaluated and updated upon change of responsibilities	1 st Line

3.4.3 Authentication and Authorization

SHUSA entities shall establish Authentication and Authorization standards to ensure that:

- Application authentication and authorization methods are appropriately risk aligned. Methods will incorporate the inherent risk of the application, the classification of the data, the risk level of the entitlement or permission (e.g., privileged vs. regular access) and the access vector (e.g., internet access, internal access).
- Anonymous access to non-public information is prohibited.
- Secure authentication credentials are established and enforced (via automated systems where possible).

Standards shall assign responsible parties for at least the following requirements:

Requirement	Accountable Unit(s)
-------------	---------------------

Ensuring access targets and systems adhere to appropriate standards for authentication and authorization through layered security and controls to appropriately address the risk attributed to the application	1 st Line
Defining the appropriate business justification (e.g., need-to-know) and related approval process for their respective information assets	1 st Line
Defining the appropriate entitlements and roles to meet least privilege and separation of duties requirements and objectives	1 st Line
Ensuring authorization processes check for separation of duty requirements	1 st Line
Development of business level roles based on job function	1 st Line
Technical provisioning of access to users based on roles	1 st Line
Technical configuration of roles and associated entitlements within an application	1 st Line

3.4.4 Attestation and Certification

SHUSA entities shall establish Attestation and Certification standards to ensure that:

- There is a defined process to confirm that workforce members' access rights (entitlements and roles) are commensurate with their assigned duties, training, and skills; and, reinforce separation of duties and least privileged principal.
- Workforce members' access rights (entitlements and roles) are reviewed after any changes to job responsibilities such as a departmental transfer.
- Review frequency is based on the risk associated with the access rights (entitlements and roles) such that high-risk transactions and privileged levels of access receive a greater frequency of review than less privileged levels of access.

Standards shall assign responsible parties for at least the following requirements:

Requirement	Accountable Unit(s)
Manage the application certification process	1 st Line

3.5 Security and Privacy Management

Security and Privacy Management addresses many of the foundational elements necessary for protecting information assets in a manner that is reasonable and appropriate for the entity operating environment. It addresses the management of policies and standards, requirements for establishing a security architecture and secure builds, data protection requirements, physical and environmental requirements, and information security training and awareness requirements.

Entity 2nd Line risk functions will ensure the following policy statements are implemented via standards:

3.5.1 Policies and Standards Management

Entities shall establish the capability for managing information risk policies and standards that implement all required internal and external mandates. The policies and standard that are developed will:

- Follow a document management life-cycle to ensure they are formally developed, approved, communicated, implemented, monitored for compliance, and periodically reviewed and updated as appropriate.
- Be developed using a risk-based approach that considers the entity operating environment, business practices, regulatory and contractual requirements, and the evolving standards for controls.
- Include an acceptable use agreement form, to be agreed to by all workforce members, that requires users to comply with all Santander policies, standards, and procedures related to information access, acceptable use, privacy, and information security. It will address unauthorized activities, prohibitions against malicious activities and unsafe computing practices, and consequences for noncompliance.

Standards shall assign responsible parties for at least the following requirements:

Requirement	Accountable Unit(s)
Drafting, publishing, communicating, monitoring for compliance, and reviewing and updating information risk policies and standards	2 nd Line
Defining and implementing processes, procedures and guidelines as necessary and appropriate to support the requirements of the information risk policies and standards	1st Line
Following processes, procedures and guidelines as necessary and appropriate to support the requirements of the information risk policies and standards	1st Line

3.5.2 Security Architecture and Secure Builds

The strategic design (i.e., Security Architecture) and desired configuration (i.e., Secure Build) of information systems (e.g., applications, operating systems, network devices) that store, process, or transmit information assets shall be documented and maintained.

Standards shall assign responsible parties for at least the following requirements:

Requirement	Accountable Unit(s)
-------------	---------------------

Designing, implementing and maintaining security architecture and secure build standards	1 st Line
--	----------------------

3.5.3 Data Protection

Entities shall develop and implement a data protection standard that defines data classification categories and the necessary security controls for each data classification. In order to promote quality enterprise-wide data protection, SHUSA will develop an enterprise-wide data protection standard to establish a set of common data classification categories and minimum expected security controls to be utilized across the enterprise. Entity-level data protection standards shall align with the enterprise-wide standard once it is published and in effect. The data protection controls will:

- Be developed using a risk-based approach that considers the entity operating environment, business practices, regulatory and contractual requirements, and the evolving standards for controls.
- Apply to information regardless of where that information is physically stored or processed, to include storage or processing by third-party service providers or business associates.
- Specify appropriate use of encryption controls and the organizational approach to key management.
- Address non-public personal information (“NPPI”) covered by privacy-related regulations and standards (e.g., 12 CFR 30 requirements, state-based privacy requirements).

Standards shall assign responsible parties for at least the following requirements:

Requirement	Accountable Unit(s)
Define data classification categories and associated security controls	1st Line
Ensure business processes consider relevant data protection controls	1st Line
Ensure applications adhere to relevant data protection controls	1st Line
Ensure training is provided on relevant data protection controls to team members	2 nd Line

3.5.4 Physical and Environmental

The controls intended to support the protection of entity information assets, workforce members and physical assets through physical controls (e.g., locks on doors, security guards, surveillance solutions) and environmental controls (e.g., heating, ventilation, air conditioning (“HVAC”), gas and electric) will be developed, approved, communicated, implemented, monitored for compliance, and periodically reviewed and updated as appropriate. The physical and environmental controls will:

- Be developed using a layered or zoned approach commensurate with the value, confidentiality, and criticality of the data stored or accessible and the identified risks.
- Consider the entity operating environment, business practices, regulatory and contractual requirements, and the evolving standards for controls.
- Address system maintenance requirements.

Standards shall assign responsible parties for at least the following requirements:

Requirement	Accountable Unit(s)
Define necessary physical and environmental controls to address information security needs	1 st Line
Ensure physical and environmental controls are incorporated into appropriate standards	1 st Line

3.5.5 Training and Awareness

The education and awareness of Workforce Members regarding information security and privacy controls, their respective roles and their responsibilities will be developed, approved, communicated, implemented, monitored for compliance, and periodically reviewed and updated as appropriate. Training and awareness campaigns will begin with training during onboarding for Workforce Members and re-enforced with periodic refreshers (e.g., email blasts, computer based training (“CBT”), targeted training sessions) as is reasonable and appropriate.

Standards shall assign responsible parties for at least the following requirements:

Requirement	Accountable Unit(s)
Define the minimum information security content needed for Workforce Member training	2 nd Line
Dissemination of the education program for Santander workforce members on their obligations and requirements for protecting information	2 nd Line
Providing notification when information risk policies or standards are changed or updated	2 nd Line
Coordinate with second line on the creation of the education program	1 st Line

3.6 Operations Management

Operations Management addresses requirements applicable to monitoring, backup, storage, network operations, security operations, and process automation capabilities.

Entity 2nd Line risk functions will ensure the following policy statements are implemented via standards:

3.6.1 Monitoring

The capability of monitoring and reporting on information systems will be implemented to allow management of system performance and capacity, identify security events, ensure the effective operation of information systems and ensure the effective operation of IT processes. Monitoring will be implemented commensurate with the risk profile of the information system. Event logging shall be sufficient to support risk-commensurate incident detection and response activities and to determine accountability for network/system activities.

Standards shall assign responsible parties for at least the following requirements:

Requirement	Accountable Unit(s)
Ensure adequate security monitoring processes are in place throughout the organization	1 st Line
Ensure individual systems are appropriately configured to meet logging requirements	1 st Line
Conduct periodic review of audit trails to identify potential security events	1 st Line
Establish retention requirements for audit trails	2 nd Line
Maintain the synchronization of system clocks	1 st Line
Manage file integrity monitoring tools for required systems	1 st Line
Ensure information systems users are appropriately notified of security	1 st Line

3.6.2 Backup and Storage

The capability of making copies or duplicate versions of information (i.e., Backup) and retaining information (i.e., Storage) to include files, configuration settings, and images of operating systems (“OS”) will be managed with a defined process. Scheduled backups or duplication of data (e.g., data replication) will be performed and storage capabilities will be in place for information systems.

Standards shall assign responsible parties for at least the following requirements:

Requirement	Accountable Unit(s)
Define application risk profile	1 st Line
Perform application backups in accordance with the application risk profile	1 st Line
Manage backups in adherence to data retention requirements	1 st Line

Routinely test backups to confirm validity	1 st Line
Ensure that necessary backup requirements are incorporated into third party service provider contracts and integrated into any due diligence processes	2 nd Line

3.6.3 Network and Security Operations

SHUSA entities shall assign responsibilities for network and security operations that will ensure the implementation of security controls and the effectiveness of those controls through measurement and reporting. SHUSA entities shall ensure that resources are appropriately dedicated to the execution of day-to-day network and security operations.

Standards shall assign responsible parties for at least the following requirements:

Requirement	Accountable Unit(s)
Implement adequate security controls to meet security standards and identified risks	1 st Line
Adequately measure security controls to ensure effectiveness	1 st Line
Conduct vulnerability scanning and penetration testing	1 st Line
Monitor the output of the vulnerability scans, penetrations tests, and other vulnerability assessments	2 nd Line
Conduct day-to-day management of network and security infrastructure (firewalls, Intrusion detection system("IDS"), Virtual private network ("VPN"), etc.)	1 st Line
Ensure Intrusion Detection Systems(IDS)/Intrusion Prevention Sysytems (IPS) are appropriately configured to meet monitoring requirements	1 st Line
Monitor or conduct periodic testing for unauthorized wireless access points	1 st Line
Manage tools to detect and prevent the spread of malicious code	1 st Line

3.6.4 Process Automation

SHUSA recognizes that systems integration and automation improves both performance and security. For this reason, entities shall identify and pursue cost-efficient and risk-commensurate opportunities to automate IT processes. IT standards shall be adopted that preference technology that integrates with automated IT processes. Common areas for process automation that shall be considered are:

- Patching
- Maintenance Processes

- Configuration Management
- Software Distribution
- Inventory System
- Incident Handling, Monitoring and Reporting
- Identity and Access Management processes (e.g., attestation and certification, single-sign on, privileged access management)

Standards shall assign responsible parties for at least the following requirements:

Requirement	Accountable Unit(s)
Ensure automation is considered upon evaluation of system and processes	1 st Line

3.7 Configuration Management

Configuration Management refers to the discipline of evaluating, coordinating, approving or disapproving, and implementing changes in hardware, software or documentation used to construct or maintain information systems. The goal of configuration management is to eliminate confusion and error brought about by changes and to maintain standardization and consistency across multiple systems.

Entity 2nd Line risk functions will ensure the following policy statements are implemented via standards:

3.7.1 Inventory and Configuration Management

SHUSA and its entities shall establish Inventory and Configuration Management standards and processes that ensure the availability of up-to-date and reliable information about information assets and the relationships between information assets that support business services. The process shall ensure use of standardized hardware and software configurations and document deviation from standard configurations. The process shall ensure that changes to information systems are properly coordinated to prevent miscommunications and errors. The process shall properly update software and hardware inventories as a result of changes and/or new deployments.

Standards shall assign responsible parties for at least the following requirements:

Requirement	Accountable Unit(s)
Maintain documentation of the Inventory and Configuration Management Process	1 st Line
Identify the scope of the configuration management process	1 st Line
Establish configuration baselines	1 st Line
Track and control changes to Configuration Items (“CIs”) within a	1 st Line

Configuration Management Database (“CMDB”)	
Ensure effective configuration management of remote equipment	1 st Line
Update the configuration management database when there is an approved change	1 st Line
Perform configuration audits	1 st Line

3.7.2 Patch Management

SHUSA and its entities shall establish a Patch Management standard and process to ensure that software patches and updates are properly identified, assessed for risk and impact, tested, and deployed as necessary and appropriate.

Standards shall assign responsible parties for at least the following requirements:

Requirement	Accountable Unit(s)
Ensuring risk-appropriate patch management processes exist for user facing applications as well as middle-layer and infrastructure level software	1 st Line
Execute patch deployment for assigned applications	1 st Line
Reporting of patch compliance	1 st Line
Maintain documentation of the Patch Management process/standard	1 st Line

3.7.3 Software Distribution

SHUSA and its entities shall control the distribution of software to user and server systems in order to ensure information access control, license tracking, and enforcement of acceptable use standards. Software distribution processes shall utilize an auditable request and approval process.

Standards shall assign responsible parties for at least the following requirements:

Requirement	Accountable Unit(s)
Establish and implement a software distribution process	1 st Line
Implement effective tracking of software licenses	1 st Line
Identify approval requirements for Applications	1 st Line
Approve access to Applications	1 st Line
Maintain documentation of Software Distribution process/standard.	1 st Line

3.7.4 Virtual Management

SHUSA and its entities shall ensure that information processed, accessed and stored on architectures utilizing virtualization technology is protected with sufficient controls such that the accepted residual risk is equivalent to that accepted for traditional architectures. Common architectures and technologies that this would apply to are Software as a Service (“SaaS”), Platform as a Service (“PaaS”) and Infrastructure as a Service (“IaaS”). This is applicable whether these services are provided in-house (private), externally (public) or a hybrid version. Additional technologies that fall into this category include virtual machines used to replace physical servers, virtual desktop infrastructure (“VDI”), and virtual storage systems. This requirement also applies to third party providers that utilize virtual technology to store, process or transmit SHUSA information.

Standards shall assign responsible parties for at least the following requirements:

Requirement	Accountable Unit(s)
Ensure risks of virtual technologies are appropriately considered as part of technology risk assessment processes	1 st Line
Ensure controls are implemented for virtual technologies such that the accepted residual risk is equivalent to that accepted for traditional architectures	1 st Line

3.8 Service Management

Service Management addresses requirements applicable to asset management, change & release management, problem & incident management, system development life cycle (“SDLC”) & software acquisition capabilities.

Entity 2nd Line risk functions will ensure the following policy statements are implemented via standards:

3.8.1 Asset Management

The capability of acquiring, operating, maintaining, upgrading, and disposing of information assets in a safe and secure fashion will be managed with a defined process. Assets will be tracked throughout their lifecycle from introduction into the operating environment through disposal.

Standards shall assign responsible parties for at least the following requirements:

Requirement	Accountable Unit(s)
Own and manage the overall asset management inventories	1 st Line
Maintain the accuracy of assigned information assets	1 st Line

Ensure that information and associated assets are appropriately classified	1 st Line
Define and periodically review access restrictions and classifications, taking into account applicable access control policies	1 st Line

3.8.2 Change & Release Management

Entities shall establish change and release management processes to assure that modifications to the computing environment will not pose undue risks and that modifications are in alignment with applicable technology standards. Such processes shall:

- Ensure risk-commensurate consideration of security requirements, training, testing, and post-change monitoring.
- Cover both routine and emergency changes to the environment.
- Specify appropriate approval requirements for changes and releases.

Standards shall assign responsible parties for at least the following requirements:

Requirement	Accountable Unit(s)
Overall ownership of the change and release management process	1 st Line
Review and approve the acquisition of all hardware, software or other technology resources and services prior to development, selection, or acquisition	1 st Line
Understand and follow change and release process procedures and requirements	1 st Line
Manage end of life tracking and the end of life process for information assets	1 st Line

3.8.3 Problem and Incident Management

The capability of identifying, analyzing, preventing and remediating problems and incidents will be managed with a defined process. Incidents will be resolved in a coordinated and controlled fashion, as expeditiously as possible, while maintaining information security considerations around confidentiality, integrity and availability. Problem and incident response processes shall define escalation procedures to be developed in coordination with IT Risk and Security.

Standards shall assign responsible parties for at least the following requirements:

Requirement	Accountable Unit(s)
Develop and maintain the incident response plan	1 st Line

Conduct incident response training & testing	1 st Line
Conduct and document post-incident analysis	1 st Line
Report information security events & suspected weaknesses through appropriate communications channels	1 st Line
Report incident to proper authorities and/or senior management	1 st Line

3.8.4 System Development Life Cycle and Software Acquisition

The process to develop and implement an information system (i.e., System Development Life Cycle) and the capabilities of selecting and purchasing software (i.e., Software Acquisition) will be managed with a defined process that considers IT and IT risk requirements. The SDLC process shall be designed in order to optimize risk avoidance (both project risk and operational risk), resource utilization and value delivery to the business.

An SDLC process shall be utilized for all software development and acquisition projects. The SDLC process shall divide the project into defined phases with work artifacts and approval requirements for each phase defined as appropriate to the IT environment and commensurate with the risk and size of the project.

Standards shall assign responsible parties for at least the following requirements:

Requirement	Accountable Unit(s)
Own and maintain the SDLC process	1 st Line
Develop procedures for outsourced development	1 st Line
Conduct source code review prior to production release	1 st Line
Implement secure coding practices that meet defined standards	1 st Line
Implement software acquisition processes that meet defined standards	1 st Line
Specify security requirement within statements of business requirements for new/enhancements to information systems	1 st Line
Implement source control security	1 st Line
Implement testing standards and integrate into SDLC process	1 st Line

4. Roles and Responsibilities

4.1 SHUSA CISO (2nd Line):

As the owner of this Policy, the SHUSA CISO authors, approves, trains, monitors and reviews the Policy. The CISO shall provide oversight and assurance that the SHUSA information risk management methodology adequately informs SHUSA policies and standards.

4.2 SHUSA Director, IT Risk and Security (1st line):

The SHUSA Director, IT Risk and Security, as a 1st line function, shall establish a risk and compliance management methodology for ensuring all regulatory and internal mandates are implemented throughout SHUSA. The Director shall:

- ensure this and related policies adequately support the SHUSA Information Security Management Program;
- conduct periodic self-assessments to measure design adequacy and operating effectiveness of requirements;
- establish a process for escalation of issues and tracking of findings; and
- develop the necessary standards to implement these policies within the SHUSA entity.

4.3 SHUSA CIO (1st line):

The SHUSA CIO shall provide pertinent information technology requirements for inclusion in this Policy and ensure IT process and functions implement this Policy (and supporting standards) through-out the IT organization.

4.4 SHUSA Chief Operational Risk Officer

Changes or updates to the Policy are developed in consultation with the CORO.

4.5 Internal Audit (3rd Line):

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

4.6 Board of Directors

The SHUSA Board shall be responsible for overseeing the development, implementation, and maintenance of SHUSA's Information Risk Management Program. 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.

4.7 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 approves the Information Risk

Management Program 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.

4.8 Enterprise Risk Management Committee

The SHUSA ERM is established under the authority of the SHUSA Risk Committee and is chaired by the SHUSA CRO. SHUSA ERM is responsible for the oversight and monitoring of all risk-taking and risk management activities across the enterprise. The SHUSA ERM reviews the Information Risk Management Program and, if necessary or appropriate, recommends to the SHUSA Risk Committee for approval the SHUSA Enterprise Information Risk Management Policy on an annual basis or on a frequency as otherwise mandated by this Policy.

4.9 SHUSA Operational Risk Management Committee

The SHUSA ERM and CRO established the SHUSA ORM to oversee operational risk. SHUSA ORM has the primary responsibility to oversee and manage the identification and monitoring of operational risk in SHUSA and its Subsidiaries. The SHUSA ORM advises the SHUSA ERM and Subsidiary Board committees on the supervision, control and reporting of Operational Risks, including Information Risk, related to Subsidiary operations and activities. The ORM oversees adherence to the Policy across the enterprise regarding Operational Risks, including Information Risk, and recommendations from internal audit, external audit, and regulators with regard to the Information Risk Management Program.

4.10 SHUSA Chief Risk Officer

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

5. Reporting Structure

As part of an overarching risk assessment and reporting program, the SHUSA Director, IT Risk and Security shall conduct periodic self-assessments to measure design adequacy and operating effectiveness of requirements specified in this Policy and within its supporting standards. The results shall be incorporated into risk reporting provided to the Chief Information Security Officer. The SHUSA Director, Information Risk and Security shall also establish a process for the escalation of issues related to this Policy.

Each entity shall establish a system for documenting findings of non-compliance this policy. The system shall document the finding, assess the risk posed by the finding, define a remediation plan, document acceptance of the plan, and track implementation of the remediation plan. Findings and their associated remediation will have explicit ownership within the organization. Entities shall have documented procedures for utilizing the findings management system.

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, ERM, SHUSA Risk Committee and/or the SHUSA Board.

7. Document History and Version Control

7.1 Ownership and Authorship

<i>Version</i>	<i>Date</i>	<i>Author</i>	<i>Owner</i>	<i>Change</i>
1.0	TBD	SHUSA CISO	SHUSA CISO	Initial Version

7.2 Sign Off

<i>Approving Body</i>	<i>Governance Committee Approval or Endorsement</i>	<i>Final Approval Date</i>
SHUSA Board	Board Risk Committee, ERM, ORM, CISO, Director, IT Risk and Security, CIO	TBD

8. Appendices

8.1 Appendix A – Key Contacts

<i>Title</i>	<i>Role</i>	<i>Name and Contact</i>
<i>SHUSA CIO</i>	<i>SHUSA IT</i>	<i>Stilianos Hillas (stilianos.hillas@santander.us)</i>
<i>SHUSA Director, IT Risk and Security</i>	<i>SHUSA ITRM</i>	<i>Frank Cignarella (Fcignarella@santander.us)</i>
<i>SHUSA CISO</i>	<i>SHUSA IRM</i>	<i>Geoff Hauge (geoffrey.hauge@santander.us)</i>

8.2 Appendix B – Regulatory Obligations Addressed by this Policy

The following are the primary regulations addressed by this Policy and supporting standards.

<i>Regulatory Agency</i>	<i>Citation</i>	<i>Title</i>
<i>OCC</i>	<i>12 CFR 30 App. B</i>	<i>Interagency Guidelines Establishing Information Security Standards</i>
<i>HHS OCR (Office for Civil Rights)</i>	<i>45 CFR 160 and 164</i>	<i>HIPAA Security and Privacy Rule Breach Notification Rules</i>
<i>Various – All State-level Enforcement Agencies</i>	<i>Various – All State-level privacy and breach notification regulations.</i>	<i>State-level privacy and breach notification regulations.</i>

In addition, SHUSA considered the following supervisory sources in developing this Policy and in its ongoing assessment and oversight of risk.

- FFIEC Audit
- FFIEC Authentication Guidance
- FFIEC Business Continuity Planning
- FFIEC Development and Acquisition
- FFIEC Information Technology Examination Handbook (IT Handbook) - Information Security
- FFIEC Management
- FFIEC Operations
- FFIEC Outsourcing Technology Services
- FFIEC Retail Payment Systems
- FFIEC_E-Banking August 2003
- FFIEC_E-Banking Supplement June 2011
- HIPAA Privacy & Breach Notification
- HIPAA Security Audit Program (OCR) - 2011
- HITECH Breach Notification Guidance and RFI (74 FR 19006)
- HITECH Breach Notification Interim Final Regulation (74 FR 42740)
- International Privacy - EU Data Protection - Safe Harbor

- International Privacy -India Information Technology (Amendment) Act 2008 and Privacy Rules
- ISO/IEC 27001:2005 - Information technology : Security techniques : Information security management systems : Requirements
- ISO/IEC 27002:2005 - Information technology - Security techniques - Code of practice for information security management
- ISO/IEC 27005 - Information technology - Security techniques - Information security risk management
- NIST 800-30 - Risk Management Guide for Information Technology Systems
- NIST 800-39 - Managing Information Security Risk
- NIST 800-66 - An Introductory Resource Guide for Implementing HIPAA Security
- Payments Card Industry Data Security Standard (PCI DSS) 2.0 - Requirements and Security Assessment Procedures
- HIPAA Omnibus Updates - Modifications to 45 CFR 160 and 45 CFR 164
- COBIT 4.1
- Dodd-Frank Act rules: § 4s (h)(23.603) (f); § 4s (h)(23.603) (g); and § 4s (h)(23.410) (h)
- FFIEC Outsource Cloud Computing
- Payments Card Industry Data Security Standard (PCI DSS) 3.0 - Requirements and Security Assessment Procedures

8.3 Appendix C – Related Policies and Process and Administrative Documents

<i>Document Type</i>	<i>Entity and Department</i>	<i>Owner</i>	<i>Document Title</i>
Policy	Operational Risk	Operational Risk	Enterprise Business Continuity and Disaster Recovery Policy
Policy	Third Party Risk Management	Third Party Risk Management	Enterprise Third Party Risk Management
Policy	Internal Audit	Internal Audit	Enterprise Audit Policy