Enhanced Audit Program

Enhanced Audit Program

Version: 3.0

Date: December 6, 2011

Table of Contents

1. Enhanced Audit Program

1.1 Overview

This document outlines the written internal audit program which has been enhanced per the requirements of the Consent Order.

1.2 Annual Audit Plan Approval

The risk assessment methodology is outlined in *Section 2100 of the SunTrust Audit Services (SAS) Internal Audit Manual*. Essentially, the risk assessment methodology and framework includes the following key components:

- Consideration of other SunTrust risk assessment efforts, management reporting and testing, external events, industry publications, and other sources as inputs into the SAS Risk Assessment process in order to facilitate an effective evaluation of risk across the organization.
- Maintenance of a comprehensive audit universe, defined at the Line of Business (LOB) and Function level as well as at the auditable unit level. The auditable units will include key control functions and key risk areas.
- Definition of risk categories as well as guidance for risk drivers, control environment, and risk rating criteria, which will help ensure comprehensive, comparable, and accurate risk ratings across auditable units.
- Assessment of risk at the LOB/Function level (top down) and the auditable unit level (bottom up).
    - Alignment of the LOB/Function risk assessment's priorities with the auditable unit risk assessments and resulting audit plan.
    - Audit strategy will detail how the audit plan addresses the priorities.
- Reporting of risk assessment, audit strategy and audit plan to facilitate prioritization and meaningful risk discussions with clients, executive management, and the Audit Committee of the Board of Directors.

Risk Categories

SAS aligns its risk assessment framework with that of the company. However, SAS has pared Financial Reporting, Compliance and Technology risk out of Operational Risk for its risk assessment. Accordingly, the six risk categories and their definitions are as follows:

- Operational - the risk of direct or indirect loss resulting from inadequate or failed internal processes, people, strategies or external events. Includes fraud risk.
- Financial Reporting Risk - the risk of unreliable or misleading financial reporting and disclosures, including to the U.S. Treasury, SEC, FDIC, (e.g., The Consolidated Report of Condition and Income, "Call Report"), FFIEC and other external reporting.

- Compliance Risk - the risk of noncompliance with federal, state and local laws, regulations, regulatory interpretations and guidance. Includes AML/BSA.
- Technology - the risk of loss due to inadequate security, confidentiality, integrity, capability or availability of systems affecting an organization's operations, assets, customers, shareholders or employees.
- Credit - the risk of default by the borrower or counterparty such that loans, bonds or leases will not be repaid on time and/or in full or the client and/or counterparty will fail to perform on an obligation to the institution (e.g. trade, OTC derivative contract).
- Market/Liquidity Risk - the risk of loss arising from adverse fluctuations in interest rates, foreign currencies, equity and commodity prices and their related volatility.

Reputation risk is a byproduct of all of the above risk categories.

LOB / Function Assessment

The LOB/Function Assessment process identifies the SAS priorities, which are the key enterprise and LOB/Function risks from an enterprise perspective that drive the SAS overall audit strategy. The LOB/Function assessment is completed in two stages: first, it is drafted by the SAS Risk Management team to provide the Managing Director teams input for their Auditable Unit Assessment (see below); second, during the Auditable Unit Assessment, the Managing Director teams assess the LOB/Function, which is used to overwrite the initial LOB/Function assessment after SAS management review, including the General Auditor.

The following are examples of inputs into the LOB/Function Assessment:

- Corporate Risk Management's assessments of risk, including:
  - Quarterly Corporate Risk Committee meeting materials that evaluate credit, market, operational, compliance, and SOX risk at the LOB and Function level.
  - Operational Risk Scenario Analyses.
  - Operational Risk and Compliance Risk and Control Self Assessments.
  - Operational Risk Metrics Dashboards.
  - Bi-annual risk management reviews of LOBs.
- LOB and Function Operational Risk Reports.
- SAS Watch List which inventories SunTrust specific risk drivers, such as new and/or changing management structure, business, product, process, system, regulation, law, rule, industry, competition, and related events.
- SunTrust specific risk drivers which may be identified through SAS continuous auditing/monitoring, including industry publications, business meetings, key initiatives, management reporting and testing.
- SunTrust strategic plan and risk tolerance.

The mortgage LOB Assessment is summarized in a heat map reflecting the six Risk Categories ratings plus an overall rating.

Auditable Unit Assessment

SAS performs the Auditable Unit Assessment. This assessment drives the audit strategy and audit plan. The Auditable Unit Assessment provides risk category definitions as well as guidance for risk drivers, control environment, and risk rating criteria, which will help ensure comprehensive and comparable risk ratings across auditable units. SAS also employs a frequency cycle based on the inherent risk ratings.

Assessing Inherent Risk

Risk Rating Criteria for each risk category are used in determining the inherent risk rating of each auditable unit. These criteria are a tool to help ensure consistency and are not meant to be all inclusive. Examples of risk rating criteria might include items such as:

- High (H) - Event requires executive management and Board attention; significant litigation and/or regulatory/legislative response; long term impact on market capitalization greater than 50%; potential jail terms or significant penalties/fines; impact to ability to conduct business (potential for Cease and Desist order); considered a core system to the proper functioning of the business or in ensuring regulatory compliance or security; sustained, serious loss in market share and market position; loss of key trading partners & customers.

- Medium (M) - Event requires senior and executive management attention, with possible Board attention; interest from governmental and/or regulatory bodies; >30% short term impact on market capitalization; potential penalties/fines; reputational risk that would affect market share, customer confidence, and brand value by a moderate amount in the short term; system not considered core and/or is not the system of record, but supports activities that ensure proper functioning of the business or in ensuring regulatory compliance or security.

- Low (L) - Issues would be dealt with by senior and executive management; event consequences can be absorbed under normal operating conditions; has little to no impact on market capitalization, market share, customer confidence, and brand value; system or process is stand-alone and does not feed or enable analysis that would affect proper functioning of the business, financial results, regulatory compliance or security.

Risk Drivers help formulate justification for the respective risk category assessment and are specific to SunTrust activities. The risk drivers are meant to serve as prompts during the inherent risk assessment process. The risk drivers are not meant to be all inclusive. Justification for the risk assessment should be supported by a brief explanation of the rationale or any significant events/trends that influence the risk category assessment.

Assessing Residual Risk

The Control Environment is considered and documented to arrive at the residual risk rating. The control environment considers items such as the results of prior audits or other testing performed, stability and maturity of people, processes, and technology, as well as changes in the control

environment (management changes, organizational changes, system changes, etc). Once the inherent risk rating is derived, the control environment is evaluated to arrive at the risk category's residual risk rating as follows: Low (L), Medium (M), High (H) and Not Applicable (N/A).

Mortgage LOB

The audit strategy and plan for the mortgage LOB are produced from the results of the LOB/Auditable Unit risk assessments, in compliance with the audit frequency guidelines and audits mandated by contract or regulation. The audit plan is based on the calendar year. The plan is developed in the Fall for the upcoming year and is presented to the Board Audit Committee for review and approval at the February Audit Committee meeting. At least quarterly, the Managing Director will review the audit plan to determine whether changes to the plan are warranted. All changes to the annual audit plan must be approved by the Audit Committee at the next regularly scheduled full-agenda meeting.

SAS will review the results of the independent risk assessment and modify audit scope and activities, if necessary.

In view of the heightened risks and the conditions of the Consent Order, SAS will add approximately 12,800 hours of auditing to the 2011 plan. The added audit activities include:

Audit	Scope
Enterprise Compliance Program over Mortgage (ECP - Mortgage)	Focus on ECP with respect to mortgage servicing, loss mitigation and foreclosure. Test processes around risk assessment, compliance with Federal Reserve SR 08-8, roles and responsibilities, Consent Order §9(a)-9(m), and documentation and audit trails.
Enterprise Risk Management over Mortgage (ERM - Mortgage)	Focus on ERM risk assessment encompassing mortgage servicing, loss mitigation and foreclosure, risk levels and trends, compliance with supervisory guidance and Consent Order §16(a)-16(l).
Vendor Management	Focus on third-party oversight, service level agreements, performance metrics, contract compliance, due diligence, certification processes, compliance with Consent Order §7(a)-7(j).
Mortgage Electronic Registration System (MERS)	Focus on system-to-system reconciliations, aging open items, corporate resolution, certifying officers, assignments and endorsements, and compliance with Consent Order §10(a)-10(g).
Management Information Systems (Servicing)	Focusing on accuracy, integrity, completeness and timeliness of MIS on servicing payment processing, payoffs, and escrow administration. Will also cover compliance with Consent Order §11(a)-11(e).

Audit	Scope
Management Information Systems (Default)	Focusing on accuracy, integrity, completeness and timeliness of MIS on Bankruptcy, Loss Mitigation and Foreclosure. Will also cover compliance with Consent Order §11(a)-11(e).
Force-Placed Insurance	Focus on processes for timely notification of clients, initiating force-placed insurance, cancellation, premium refunding, vendor management.
Issue Management & Continuous Control Assessment in Servicing	Focus on following up and confirming closure of audit issues, MRAs, and Consent Order compliance. Additionally, develop continuous control assessment over payment processing and escrow administration.

Accordingly, the adjusted 2011 audit plan for SunTrust Mortgage is below. The scope and timing of some of the "added" audits depends on when action plans to comply with the Consent Order are completed. For example, SAS will conduct an audit of Vendor Management in Q4 of 2011 and issue the report by February 2012. However, the exact scope of the Vendor Management audit will depend on how far along management is in completing their action plans. SAS will monitor the progress of Consent Order actions on an ongoing basis, through specific audit work in the applicable areas and by attending progress status meetings.

Current 2011 Plan	Additions
Origination – Correspondent	Mortgage Electronic Registration System
Origination – Wholesale	Vendor Management
Origination – Reverse Mortgages	Enterprise Risk Management
Origination – Joint Ventures	Enterprise Compliance Program
Servicing – Client Contact Center	Default Management Information Systems
Servicing – Government Insuring (FHA/VA)	Servicing Management Information Systems
Servicing – Warehouse & Production Operations	Force-Placed Insurance
Servicing – Investor Reporting	Continuous Auditing of Servicing
Servicing – Payment Processing & Payoff	Consent Order Compliance & Follow Up
Default – Foreclosure	
Default – Loss Mitigation	
Default – Recovery	
Default – Continuous Auditing Loss Mitigation	
Quality Control	
Mortgage Servicing Technology	
Asset Management	
Secondary Marketing & Pipeline	
Mortgage Servicing Rights (MSR)	

Current 2011 Plan	Additions
Client Centric Origination Project (CCO)	
[redacted] Project	
Dodd-Frank Controls	
State of Control	
Issue Follow Up	

1.3 Scope & Frequency

The risk-based planning model for SunTrust Mortgage will evolve from a three-year frequency cycle to a two-year cycle given heightened risks in mortgage operations and the escalated volume of control deficiencies and issues. This change in frequency will result in all mortgage activities being audited at least every other year, and many areas audited annually. SAS will conduct annual audits of key servicing, loss mitigation and foreclosure (SLMFC) activities such as collections, loss mitigation, foreclosure, bankruptcy, MERS, payment processing, and investor reporting. Once the remediation efforts to comply with the Consent Order are completed and functioning effectively, the frequency cycle for SunTrust Mortgage will return to the normal three-year cycle.

The initial scope of each audit is defined in the announcement memo emailed to the auditee at the start of each engagement. Initial scopes may be fine-tuned during the planning process in view of new information and data received during the normal course of business. In planning an audit engagement, SAS gains a comprehensive understanding of the processes and activities under review, along with the identification of key risks and controls. SAS evaluates risk in six categories: credit risk, market risk, operational risk, financial reporting risk, compliance risk and technology risk. These key risks are recorded in a risk assessment document and serve to provide a clear outline of the audit scope.

1.4 Independence of Internal Audit

SunTrust Audit Services (SAS) is an independent and objective corporate assurance function. SAS fully complies with the *Institute of Internal Auditors* (IIA) Standards 1110 and 1110.A1, which require internal audit activity to be free from interference in determining the scope of internal auditing, performing work, and communicating results. The standards also require the chief audit executive to report to a level within the company that allows internal audit to fulfill its responsibilities.

The SAS General Auditor functionally reports to the Audit Committee of SunTrust's Board of Directors and administratively to the General Counsel. The operations and activities of SAS are overseen by the Board Audit Committee. SAS auditors comply with the *IIA International Standards for the Professional Practice of Internal Auditing* and associated *IIA Code of Ethics*. SAS auditors also conform to the SunTrust *Code of Business Conduct and Ethics* and comply with the standards outlined in the SAS *Internal Audit Manual.*

The Audit Committee is appointed by the Board of Directors of SunTrust Banks, Inc. The Audit Committee's authority and responsibility is outlined in a written charter. Each Committee member must meet the independence and financial literacy requirements of the New York Stock exchange

Listed Company Manual Rules 303A.02 and 303A.07, Section 10A(m)(3) of the Securities Exchange Act of 1934.

1.5 Inclusions in Audit Scope

The annual audit plan for SunTrust Mortgage provides for testing of internal controls, management information systems, and compliance with policies and procedures. Audits of Servicing and Default (collections, bankruptcy, loss mitigation, foreclosure) will include assessments and testing of internal controls, compliance with policies and procedures, and the adequacy of management reports. Specific audits of data integrity and management information systems in Servicing and Default have been added to the 2011 audit plan, and will be regularly audited thereafter.

1.6 Management Information Systems (MIS)

SAS will conduct audits of management information systems (MIS) in Servicing and Default. Audits of Default MIS will occur annually.

To expand on the scope highlighted on pages 6 and 7, the MIS audits will cover data integrity, data transmission/movement, disaster recovery, data security and system-to-system and general ledger reconciliations. Additionally we will look at the accuracy and sufficiency of operational and executive management reporting.

1.7 Compliance with Legal Requirements

SAS risk-based audits will include testing of compliance with applicable and material legal requirements. During the course of the audit frequency cycle, testing for compliance with legal requirements will include, at a minimum, the following:

11 USC §362 (U.S. Bankruptcy Code)	12 CFR 202 (Regulation B)
12 USC §4901 (Homeowners Protection Act	12 CFR 22 (Flood Disaster Protection Act)
12 USC §4902 (Private Mortgage Insurance)	12 CFR 226 (Regulation Z)
15 USC §1692 (Fair Debt Collections Practices)	24 CFR 3500 (Real Estate Settlement Procedures)
50 USC §527 (Servicemember Civil Relief Act)	12 CFR 227 (Unfair and Deceptive Practices Act)
15 USC §1681 (Fair Credit Reporting)	12 CFR 208 Appendix D (Safety & Soundness)
Home Affordable Modification Program Directives	Contract Compliance
MERS Membership Rules	Federal Reserve SR Letters (applicable)
HUD Handbooks (FHA Lending)	Fannie Mae Servicing Guide
Veterans Administration Lender's Handbook	Freddie Mac Servicing Guide
State Foreclosure Laws	State Notary Requirements

SAS has engaged KPMG and is working with legal counsel to develop guidance documents and testing templates for auditing compliance with each state's foreclosure requirements. SAS will also

engage legal counsel on an ongoing basis to inform SAS on new laws or regulations or changes to laws and regulations. Such information will be used in the planning of specific audit engagements.

1.8 Timely Completion of Audits

It is SAS's goal and intent to complete the annual audit plan by February of the following year. SAS will ensure sufficient resources to accomplish this annual goal by adding co-source resources when necessary. Additionally, at the beginning of each audit engagement SAS will establish target dates for key milestones such as the completion of the risk assessment matrix, which is used to document risks and controls in the area or process under review. Target dates will also be set for the timely issuance of both draft and final audit reports to management.

SAS Project Managers and Quality Reviewers will set expectations and target dates for the engagement team. The SAS Director will monitor performance throughout the project to identify and resolve any bottlenecks. Benchmarks or metrics for assessing the timeliness of completion of key milestones will be established. Reports will be developed to track progress and report on results. These reports will be distributed to and reviewed by Project Managers, Quality Reviewers, and the SAS Director.

1.9 Staffing

During 2010, in response to a Federal Reserve examination of the SAS internal audit function, KPMG performed a review of the organization structure and staffing of SAS. In addition KPMG developed job criteria for each line of business audit managing director, including the mortgage audit team. This criterion was compared to the experience and background of the audit managing directors to ensure they had the requisite qualifications, skills and ability to perform their function. Specifically, for the mortgage audit team, while the audit managing director met or exceeded all of the job criteria, it was determined that staffing levels needed to be increased from six auditors at the beginning of 2010 to thirteen by the end of 2010.

In response to this Order, SAS will increase the staffing level to twenty in 2011 and re-evaluate staffing on a quarterly basis in accordance with the Division's risk assessment methodology. SAS will also engage external co-source resources to provide subject matter expertise, as necessary. SAS will review the results of the independent foreclosure review and risk assessment and adjust staffing and audit plans, if necessary.

In response to prior issues identified by the Federal Reserve Bank, an independent consultant (KPMG) performed an analysis of the adequacy and qualifications of staff in the audit function. That analysis was presented to the Board Audit Committee in August 2010. SAS will have KPMG refresh the staffing analysis post-implementation of new audit activities to comply with Consent Order requirements.

Almost half (46%) of the current audit staff assigned to the mortgage company have over 20 years of auditing experience. All auditors are college graduates with at least a bachelor's degree, and most (80%) have earned professional certifications such as Certified Public Accountant, Certified Internal Auditor, or Certified Information Systems Auditor. SAS's training guidelines call for auditors to receive an average of 40 hours of training each year.

1.10 Tracking & Reporting of Audit Findings

Section 3300 of the SAS Internal Audit Manual addresses the disposition of action plans developed by management to resolve issues identified by the audit. SAS monitors and reports on the status of outstanding audit issues on a monthly basis. Additionally, when management reports the completion of an action plan, SAS will evaluate the corrective action to ensure management has addressed the issue and mitigated the risk to an acceptable level.

SAS will implement a new process and SharePoint web site for tracking the current status and resolution of audit findings. Owners and responsible parties on issues will be required to access the site monthly and provide updates on the status and progress of action plans. Supporting documentation evidencing the completion of action plans will also be captured on the site. Summary reports will be provided to the Audit Committee. This new process and web site for sharing information will ensure that SAS and the Audit Committee are kept informed of the status of all issues and action plans. Audit reports, issues and the status of action plans in SunTrust Mortgage will be reported to the Audit Committee quarterly.

Section 3302 of the SAS Internal Audit Manual addresses follow-up reviews to ensure the completion and effectiveness of corrective measures. Upon being informed that an action plan has been completed, SAS will review the completed action plan and any documentation provided. Depending upon the nature of the issue and its rating, SAS will select the appropriate validation strategy for confirming the issue closure. Such strategies can range from reviewing documentation and interviewing stakeholders to re-testing. It is SAS's policy to determine whether or not an action plan can be closed within 60 days of receiving notice that the action plan is completed.

1.11 Escalation Process

Section 3310 of the SAS Internal Audit Manual addresses the process for escalating differences of opinion between SAS and management on audit findings. SAS obtains action plans from management at the time the audit report is issued. Action Plans can be grouped into four categories:

- *Avoid* – management may choose to exit or divest of the activities giving rise to the risk.
- *Reduce* – management may implement controls to reduce the likelihood and/or impact of the risk.
- *Share* – management may reduce the likelihood or impact of the risk by transferring or sharing it (e.g., purchase insurance, hedging).
- *Accept* – management may choose to take no action.

Pursuant to *Section 3310*, when SAS concludes that management has accepted a level of residual risk that does not align with the SunTrust policies, risk appetite, or laws and regulations, the SAS Managing Director and Chief Audit Executive will discuss the matter with executive management. If it is not satisfactorily resolved, the Chief Audit Executive and Line of Business Head will then present the significant matter to the Audit Committee for resolution.

2. Glossary

Acronym	Definition
AML/BSA	Anti money laundering / Bank Secrecy Act
ECP	Enterprise-wide Compliance Program over servicing, loss mitigation & foreclosure
ERM	Enterprise-wide Risk Management over servicing, loss mitigation & foreclosure
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FHA	Federal Housing Administration
IIA	Institute of Internal Auditors
MERS	Mortgage Electronic Registration System
MIS	Management information systems
MSR	Mortgage servicing rights
LOB	Line of business
OTC	Over the counter
SAS	SunTrust Audit Services
SEC	Securities and Exchange Commission
SOX	Sarbanes-Oxley
VA	Veterans Administration