

DEPARTMENT OF SAVINGS AND MORTGAGE LENDING
Austin, Texas

ANNUAL INTERNAL AUDIT REPORT

Fiscal Year 2016



DEPARTMENT OF SAVINGS AND MORTGAGE LENDING
Austin, Texas

Annual Internal Audit Report
Fiscal Year 2016

TABLE OF CONTENTS

	<u>Page</u>
Internal Auditor's Report.....	1
Introduction.....	2
Internal Audit Objectives.....	3
Executive Summary	
Management Information Systems	
Background.....	4-6
Audit Objective, Scope, and Methodology.....	6-8
I. Compliance with Texas Government Code 2102: Required Posting of Internal Audit Information	9
II. Internal Audit Plan for Fiscal Year 2016	10
III. Consulting and Nonaudit Services Completed	10
IV. External Quality Assurance Review	10
V. Observations/Findings and Recommendations	11-14
VI. External Audit Services Procured in Fiscal Year 2016.....	15
VII. Reporting Suspected Fraud and Abuse	15
VIII. Proposed Internal Audit Plan for Fiscal Year 2017	15
IX. Organizational Chart	16

Garza/Gonzalez & Associates

CERTIFIED PUBLIC ACCOUNTANTS

Finance Commission Members and
Audit Committee Members
Department of Savings and Mortgage Lending
Austin, Texas

We performed tests of management's assertion about the effectiveness and efficiency of the Department of Savings and Mortgage Lending's (SML) internal control structure over the Management Information Systems (MIS) area and its established policies and procedures, as applicable to the MIS area, for the purpose of determining SML's compliance with selected requirements of the Texas Administrative Code (TAC) Chapter 202, the Texas Government Code (TGC) Chapter 2054; and, selected control groups from the Security Control Standards Catalog Version 1.3 (Control Catalog), for the 9 months ended May 31, 2016.

The results of our tests disclosed that SML's internal control structure over the MIS area and its established policies and procedures, as applicable to compliance with the selected requirements of TAC 202, TGC 2054, and the selected control groups from the Control Catalog, were generally adequate and no material instances of noncompliance were noted; however, we noted a certain matters, included in this report, that are opportunities for strengthening internal controls and ensuring compliance with state requirements and SML's established policies and procedures. We also performed a follow-up of the findings that were presented in the prior year annual internal audit report and this report reflects the implementation status of those matters; and, includes all information required for the State of Texas Internal Audit Annual Report requirements.

We have discussed the comments and recommendations from the MIS area audit; and, the implementation status from the follow-up performed, with various SML personnel; and, will be pleased to discuss them in further detail; to perform an additional study of these matters; or, to assist you in implementing the recommendations.



July 25, 2016

DEPARTMENT OF SAVINGS AND MORTGAGE LENDING

Annual Internal Audit Report
Fiscal Year 2015

INTRODUCTION

The Department of Savings and Mortgage Lending (SML) has 2 key areas of regulatory responsibility, the chartering, regulation and supervision of the state's thrift industry; and, the licensing/registration and regulation of the state's mortgage industry. These 2 areas of responsibility cover the vast majority of residential mortgage lending in Texas.

The 58th and 73rd Legislatures, respectively, enacted the Texas Savings and Loan Act and the Texas Savings Bank Act for the chartering, regulation, examination and supervision of state chartered savings banks and savings and loan associations and enforcement of these statutes.

The 76th Legislature enacted the Mortgage Broker License Act for licensing and regulation of first lien residential mortgage brokers and loan officers doing business in Texas. The statute, as amended by the 80th Legislature, applies to all residential mortgages regardless of lien position. The statute prescribes requirements for licensing and inspecting licensees, and processing consumer complaints.

The 78th Legislature enacted the Mortgage Banker Registration Act for registering mortgage bankers conducting business in Texas and providing their borrowers with notice of the process for filing consumer complaints.

The 81st Legislature enacted the Texas SAFE Act (Chapter 180) and other significant modifications to Chapters 156 and 157 of the Texas Finance Code. Compliance with the federal mandates addressed by this legislation expanded the field of individuals subject to residential mortgage licensing.

The 82nd Legislature enacted Senate Bill 17 creating Chapter 158 of the Texas Finance Code calling for the registration of non-depository third party residential mortgage loan servicers. The statute authorizes SML to require registrants to carry a bond or equivalent, and to notify borrowers whose loans they service of the borrower's ability to file a complaint with SML. Additionally, the statute authorized SML to investigate any such complaints. SML is not authorized to initiate examinations of servicing registrants but may participate in multistate examinations.

SML was granted Self-Directed, Semi Independent (SDSI) status in the 81st Legislative Session. As an SDSI agency, SML is not required to have its budget approved by the Legislature; however, the Finance Commission is responsible for setting SML's spending authority or limits. SML's entire operating funds are generated from fees assessed to regulated entities and are used to fund both direct and indirect costs. General revenue funds are not used to support SML's operations.

2016 Internal Audit Plan

Following are the internal audits and other functions performed, as identified in SML's approved 2016 Internal Audit Plan:

- Management Information Systems
- Follow-up of Prior Year Internal Audits
- Other Tasks

This report contains the results of our audit of the Management Information System area, reflects the follow-up performed in the current year, and meets the State of Texas Internal Audit Annual Report requirements.

DEPARTMENT OF SAVINGS AND MORTGAGE LENDING

Annual Internal Audit Report

Fiscal Year 2016

INTERNAL AUDIT OBJECTIVES

In accordance with the **International Standards for the Professional Practice of Internal Auditing**, the audit scope encompassed the examination and evaluation of the adequacy and effectiveness of SML's system of internal control and the quality of performance in carrying out assigned responsibilities. The audit scope included the following objectives:

- **Reliability and Integrity of Financial and Operational Information** – Review the reliability and integrity of financial and operating information and the means used to identify, measure, classify, and report such information.
- **Compliance with Policies, Procedures, Laws, Regulations, and Contracts** – Review the systems established to ensure compliance with those policies, procedures, laws, regulations, and contracts which could have a significant impact on operations and reports, and determine whether the organization is in compliance.
- **Safeguarding of Assets** – Review the means of safeguarding assets and, as appropriate, verify the existence of such assets.
- **Effectiveness and Efficiency of Operations and Programs** – Appraise the effectiveness and efficiency with which resources are employed.
- **Achievement of the Organization's Strategic Objectives** – Review operations or programs to ascertain whether results are consistent with established objectives and goals and whether the operations or programs are being carried out as planned.

DEPARTMENT OF SAVINGS AND MORTGAGE LENDING

Annual Internal Audit Report

Fiscal Year 2016

EXECUTIVE SUMMARY

Management Information Systems (MIS)

Background

The Information Technology Department (Department) is responsible for the Management Information Systems (MIS) area, and has the primary responsibility for ensuring confidentiality, integrity, and availability of SML's information resources. The statutory requirements, related to information resources, are outlined in Texas Government Code (TGC) Chapter 2054, the Information Resources Management Act; and, the administrative rules are detailed in Title 1, Part 10 of Texas Administrative Code Chapter 202 (TAC 202), the Information Security Standards.

The Department is comprised of a Director, who reports directly to the Commissioner, and a system support specialist; however, this position has been vacant since March 31, 2016. In accordance with TGC §2054.071 and TAC §211.10, the Director was designated as SML's Information Resources Manager (IRM); and, in accordance with TAC §202.20(1), was also designated as SML's Information Security Officer (ISO).

The responsibilities of the Department include: operation and maintenance of the servers, administrative and technical support for SML's network and telecommunication systems; software and hardware upgrades; information security; and, strategic planning.

External Security Controls

SML utilizes a virtual private network, which allows employees to securely connect through encrypted connections to SML's servers from offsite locations. SML also utilizes a third party email system from ZixCorp, which allows emails to be secure and enables, but does not necessarily require, emails to be encrypted. ZixCorp analyzes outgoing emails for sensitive or confidential information; such as, social security numbers, and routes the email as a secure email, which requires the recipient to register and log in to obtain the email. Users may also manually flag emails to be encrypted.

Physical Security Controls

Critical hardware; such as, servers, routers, switches, firewalls and related software applications are located in a locked room, where a numbered key code is required for entry. Servers are connected to UPS battery backup devices, which would continue to operate in the event of a power loss. The locked room is equipped with a fire extinguisher, a fire detector, and an external air conditioner.

Backup Procedures

SML's network data is backed up nightly to the server and to an external hard drive. The backup contains files, emails and database server backups. Every Tuesday the external hard drive is picked up by the Texas State Library and Archives Commission for storage. Backups are tested periodically for reliability, through retrieval of files or migration of files to new hardware.

DEPARTMENT OF SAVINGS AND MORTGAGE LENDING

Annual Internal Audit Report

Fiscal Year 2016

Passwords

All desktops/laptops are protected through either 128 bit or 256 bit encryption and require unique passwords to gain access and to limit access to authorized individuals. This logon also grants a person access to the network and corresponding SML servers; and, is controlled through the Windows Server Active Directory. Password requirements take into account complexity, length, history, and expiration. Each software application requires a logon and password to gain access. To further prevent unauthorized access, desktops/laptops that are unattended for fifteen (15) minutes lock and require reentry of the password.

Applications

The following are the major applications currently used by SML—

- *My License (Semarca)* – a legacy database that was developed and is supported by a third party vendor for SML; and, contains information for licensing, examinations, and enforcement regarding applicants and licensees.
- *National Multistate Licensing System & Registry (NMLS)* – a national licensing database that is owned and supported by the State Regulatory Registry.
- *Application Extender* – an imaging system purchased along with the Department of Banking (DOB) and the Office of Consumer Credit Commission (OCCC); and, maintained by DOB.
- *SAGE Fund Accounting* – an internal accounting system purchased by SML.
- *USAS & USPS* – Texas Comptroller's Office accounting and payroll systems.

User Access/Termination

When an employee is hired or terminated, a Security Access Request Form is completed by the Human Resources Department and sent to the Department to add or remove access to email, network, application extender, and other programs. The Department grants access to an employee based on the respective job title and locks out the employee when an employee is terminated and then disables their account.

Desktops/laptops that are to be disposed of as state surplus property have their data erased utilizing a third party software. This software essentially writes over the hard drive several times thereby making sensitive data recovery unlikely.

Subsequent Event

In May 2016, SML contracted with a third-party information technology managed services vendor that will be responsible for managing SML's network, providing help desk operations, performing backups, hosting and securing data, and managing hardware needs.

DEPARTMENT OF SAVINGS AND MORTGAGE LENDING

Annual Internal Audit Report

Fiscal Year 2016

TAC §202

TAC §202 underwent a major revision effective March 2015, in accordance with the 40 TexReg 1357.

Following are key revisions to TAC §202:

- Clarifies the roles and responsibilities for an agency head related to information security.
- Provides details on the responsibilities for the agency's designated ISO.
- Clarifies the security responsibilities of state agency staff who own, have custody of, or use information resources.
- Highlights the required reporting of security incidents and the biennial security plan to the DIR; and the agency ISO's annual report on security policies, procedures and practices to the agency head.
- Requires each agency to perform and document a risk assessment of its information and information systems, and assess levels of risk on its mission and function.
- Establishes and mandates compliance with a Securities Control Standards Catalog (Control Catalog) published by the DIR, which provides state agencies guidance for implementing security controls in a format that easily aligns with the National Institute of Standards and Technology.

To minimize the impact to state agencies in implementing the requirements of the Control Catalog, DIR has sequenced the implementation deadlines for the various controls to be phased in over a 3 year period. As such, controls already addressed prior to the revision were required to be implemented by February 2015; and, the remaining requirements, dependent on the priority assigned by DIR to each requirement, will be phased in by February 2017.

AUDIT OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The objective of our audit was to determine whether SML's policies, procedures and processes in place, as applicable to the MIS area, are sufficient in ensuring compliance with selected requirements of TAC §202 and TGC §2054; selected control groups from the Control Catalog (version 1.3); and with other requirements imposed on state agencies by the DIR and/or other oversight agencies.

Scope

The scope of our audit was to determine SML's compliance with selected requirements of TAC §202; to include, selected controls from the Control Catalog that were required to be implemented by February 2016; selected requirements of TGC §2054; and, other requirements as mandated by the DIR and/or other oversight agencies, for the 9 months ended May 31, 2016.

DEPARTMENT OF SAVINGS AND MORTGAGE LENDING

Annual Internal Audit Report

Fiscal Year 2016

Methodology

The audit methodology included a review of policies and procedures, and other internal and external documentation; an interview and correspondence with the MIS Department's personnel; and, an onsite walk-through.

We obtained and/or reviewed the following documentation:

- a. SML's current IT policies and procedures.
- b. An illustration of SML's network diagram.
- c. MIS Department organizational chart.
- d. Vulnerability assessment dated November 20, 2015, performed by DIR.
- e. SML's business continuity plan.
- f. A listing of SML's systems and applications.
- g. An IT inventory listing.
- h. A listing of SML employees which included the date of hire and date of termination that occurred during the period from September 1, 2015 through May 31, 2016.
- i. Monthly incident reports submitted to the DIR for the months of September 1, 2015 through April 30, 2016.
- j. An active directory listing with user's current status.

We performed various procedures, to include the following:

- a. Obtained an understanding of legal and regulatory requirements relevant to SML's information resources management through review of laws and regulations; and, SML's IT policies and procedures.
- b. Reviewed third party assessment reports listed above to identify potential areas of concern.
- c. Reviewed the controls and processes in place, and interviewed with the MIS Department's personnel to evaluate whether SML has established and implemented selected controls outlined in the Control Catalog that were due for implementation by February 2016. We reviewed the security controls associated with the following areas:
 - (1) Encryption requirements for storage devices, data transmission, portable devices, etc.
 - (2) Addition, modification and deletion of user access to the information resources.
 - (3) Audit and accountability for changes made to the information resources.
 - (4) Password settings (complexity, history, change interval).
 - (5) Physical security over information resources.
 - (6) Data backup and disaster recovery.

DEPARTMENT OF SAVINGS AND MORTGAGE LENDING

Annual Internal Audit Report

Fiscal Year 2016

- d. Reviewed the controls and processes in place to ensure sensitive or confidential information is protected from unauthorized access, modification, or destruction.
- e. Reconciled current network users from the active directory listing with current SML employees to ensure only legitimate active accounts existed.
- f. Selected all terminated employees from the listing of SML employees to determine whether user access was removed in a timely manner and whether a Security Access Request Form was properly completed.
- g. Conducted physical observations of MIS hardware to ensure proper safeguards are in place.
- h. Obtained an understanding of the reporting requirements outlined in the TAC §202 and ensured SML's compliance with the reporting submission requirements.
- i. Reviewed the IRM's continuing professional education (CPE) record to ensure compliance with DIR's requirements specified in the IRM Continuing Education Guide.

DEPARTMENT OF SAVINGS AND MORTGAGE LENDING

Annual Internal Audit Report

Fiscal Year 2016

I. Compliance with Texas Government Code 2102: Required Posting of Internal Audit Information

To comply with the provisions of Texas Government Code, 2102.015 and the State Auditor's Office, within 30 days after approval by the Finance Commission, SML will post the following information on its website:

- An approved fiscal year 2017 audit plan, as provided by Texas Government Code, Section 2102.008.
- A fiscal year 2016 internal audit annual report, as required by Texas Government Code, Section 2102.009.

The internal audit annual report includes any weaknesses, deficiencies, wrongdoings, or other concerns raised by internal audits and other functions performed by the internal auditor as well as the summary of the action taken by SML to address such concerns.

II. Internal Audit Plan for Fiscal Year 2016

The Internal Audit Plan (Plan) included one audit to be performed during the 2016 fiscal year. The Plan also included a follow-up of the prior year audit recommendations, as applicable, other tasks as may be assigned by the Finance Commission, and preparation of the Annual Internal Audit Report for fiscal year 2016.

Risk Assessment

Utilizing information obtained through the inquiries and background information reviewed, 14 audit areas were identified as potential audit topics. A risk analysis utilizing our 8 risk factors was completed for each individual audit topic and then compiled to develop an overall risk assessment.

Following are the results of the risk assessment performed for the 14 potential audit topics identified:

HIGH RISK	MODERATE RISK	LOW RISK
Legal and Enforcement	Financial Reporting	Payroll and Human Resources
Thrift Examinations		Mortgage Licensing and Registration
Mortgage Examinations		Records Management
Thrift Supervision and Compliance		Consumer Protection
Revenue Accounting Process		Fixed Assets
Purchasing and Travel		Risk Management
Management Information Systems		

DEPARTMENT OF SAVINGS AND MORTGAGE LENDING

Annual Internal Audit Report

Fiscal Year 2016

In the prior 3 years, internal audits were performed in the following areas:

Fiscal Year 2015:

- Mortgage Examinations

Fiscal Year 2014:

- Consumer Protection

Fiscal Year 2013:

- Thrift Supervision and Compliance

The area recommended for internal audit and other tasks to be performed for fiscal year 2016 were as follows:

<u>Report No.</u>	<u>Audits/Report Titles</u>	<u>Report Date</u>
1.	Management Information Systems	7/25/2016
1.	Annual Internal Audit Report – Follow-Up of Prior Year Internal Audits	7/25/2016
-	Other Tasks Assigned by the Finance Commission	None

III. Consulting and Nonaudit Services Completed

The internal auditor did not perform any consulting services, as defined in the Institute of Internal Audit Auditors' *International Standards for the Professional Practice of Internal Auditing* or any non-audit services, as defined in the *Government Auditing Standards, December 2011 Revision*, Sections 3.33-3.58.

IV. External Quality Assurance Review

The internal audit department's most recent *System Review Report*, dated October 7, 2015, indicates that its system of quality control has been suitably designed and conforms to applicable professional standards in all material respects.

DEPARTMENT OF SAVINGS AND MORTGAGE LENDING
 Annual Internal Audit Report
 Fiscal Year 2016

V. Observations/Findings and Recommendations

Report No.	Report Date	Name of Report	Observations/Findings and Recommendations	Status (Implemented, Partially Implemented, Implementation Delayed, No Action Taken, Do Not Plan to Take Corrective Action, or Other)	Fiscal Impact/Other Impact
1	7/25/2016	MIS	<p>1. Disaster Recovery Plan</p> <p>DIR's Security Control Standard Catalog's Contingency Plan (CP-2)(d) states that each state organization shall maintain a written disaster recovery plan for major or catastrophic events that deny access to information resources for an extended period; and, will include the following:</p> <ul style="list-style-type: none"> a. Contain measures which address the impact and magnitude of loss or harm that will result from an interruption; b. Identify recovery resources and a source for each; c. Contain step-by-step implementation instructions; and, d. Include provisions for annual testing. <p>In October 2014 SML developed a Continuity of Operation Plan (COOP), which replaced its disaster recovery plan; however, the COOP does not include a disaster recovery plan or any of the above listed requirements.</p> <p>Recommendation We recommend that SML develop or update the previous disaster recovery plan to comply with DIR's Security Control Standards Catalog CP-2(d).</p> <p>Management's Response In addition to the COOP, the Department has a disaster recovery plan which needs updating. As the Department moves forward with the use of the contracted vendor amendments will be made to update the plan as needed to accommodate these changes and to ensure compliance with the Security Control Standards.</p>		To ensure compliance with DIR's Security Control Standard Catalog.

DEPARTMENT OF SAVINGS AND MORTGAGE LENDING
 Annual Internal Audit Report
 Fiscal Year 2016

Report No.	Report Date	Name of Report	Observations/Findings and Recommendations	Status (Implemented, Partially Implemented, Implementation Delayed, No Action Taken, Do Not Plan to Take Corrective Action, or Other)	Fiscal Impact/Other Impact
1	7/25/2016	MIS	<p>2. Risk Assessments</p> <p>TAC §202.25 requires state agencies to perform and document a risk assessment of the agency's information resources and update the risk assessment based on the agency's inherent risk. The inherent risk and frequency of the risk assessment will be ranked, at a minimum, as either "High," "Moderate," or "Low." DIR's Security Control Standards Catalog suggest that risk assessments be performed annually.</p> <p>SML has not performed a risk assessment, but plans to contract a third party vendor to perform the risk assessment, as recommended by DIR.</p> <p>Recommendation We recommend that SML continue with their plan to contract a third party vendor to conduct the risk assessments to be compliant with TAC §202.25.</p> <p>Management's Response The Department, as indicated during the audit, has been working with a third party vendor, contracted with by DIR, to conduct the required risk assessment for state agencies. Since the audit fieldwork, the contract has been finalized and the work is scheduled to begin in late Fall.</p>		To ensure compliance with TAC §202.

DEPARTMENT OF SAVINGS AND MORTGAGE LENDING
 Annual Internal Audit Report
 Fiscal Year 2016

Report No.	Report Date	Name of Report	Observations/Findings and Recommendations	Status (Implemented, Partially Implemented, Implementation Delayed, No Action Taken, Do Not Plan to Take Corrective Action, or Other)	Fiscal Impact/Other Impact
1	7/25/2016	MIS	<p>3. Audit Trails</p> <p>DIR's Security Control Standards Audit Events (AU-2) states that information resources systems shall provide the means whereby authorized personnel have the ability to audit and establish individual accountability for any action that can potentially cause access to, generation of, modification of, or affect the release of confidential information.</p> <p>In addition, it states that appropriate audit trails shall be maintained to provide accountability for updates to mission critical information, hardware and software, and for all changes to automated security or access rules.</p> <p>Our testing and discussions with the Director indicated that such audit trails are currently not in place.</p> <p>Recommendation We recommend SML request that the 3rd party vendor who is currently managing SML's IT functions, ensure such audit trails are established and able to be reviewed by the Director, as needed.</p> <p>Management's Response The Department agrees with the recommendation and will work towards complying with the Security Control Standards Audit Events requirement.</p>		To ensure compliance with DIR Security Control Standards.

DEPARTMENT OF SAVINGS AND MORTGAGE LENDING
 Annual Internal Audit Report
 Fiscal Year 2016

Report No.	Report Date	Name of Report	Observations/Findings and Recommendations	Status (Implemented, Partially Implemented, Implementation Delayed, No Action Taken, Do Not Plan to Take Corrective Action, or Other)	Fiscal Impact/Other Impact
1	7/25/2016	2016 Follow-Up	<p>Follow-Up of Prior Year Audits</p> <p>Following is that status of the recommendations made during fiscal year 2015 that had not been implemented.</p> <p><u>Mortgage Examinations</u></p> <p>1. Scheduling of Mortgage Examinations</p> <p>Our testing of mortgage banker and company examinations disclosed instances where the examinations were conducted after the required time period required by the Exam Manual.</p> <p>We recommended that SML strengthen their controls to ensure examinations were performed in a timely manner, as prescribed by procedures documented in the Area's Exam Manual(s).</p>	Implemented	

VI. External Audit Services Procured in Fiscal Year 2016

SML procured the internal audit services documented in the Internal Audit Plan for fiscal year 2016.

VII. Reporting Suspected Fraud and Abuse

SML has provided information on their home page on how to report suspected fraud, waste, and abuse to the State Auditor's Office (SAO) by posting a link to the SAO's fraud hotline. SML has also developed a Fraud Prevention Policy that provides information on how to report suspected fraud.

VIII. Proposed Internal Audit Plan for Fiscal Year 2017

The risk assessment performed during the 2016 fiscal year was used to identify the following *proposed* area that is recommended for internal audit and other tasks to be performed for fiscal year 2017. The Internal Audit Plan for Fiscal Year 2017 will be developed and presented to the Finance Commission at a meeting to be determined at a later date.

- Financial Reporting
- Follow-up of Prior Year Internal Audits
- Other Tasks Assigned by the Finance Commission

DEPARTMENT OF SAVINGS AND MORTGAGE LENDING

Annual Internal Audit Report

Fiscal Year 2016

IX. Organizational Chart

