Dovenmuehle Mortgage, Inc.

SOC 1 Type 2 Report

Report on the Subservicing Operations System Throughout the Period from October 1, 2019 to September 30, 2020

plante moran | Audit. Tax. Consulting. Wealth Management.

Contents

Plante & Moran, PLLC
10 South Riverside Plaza
9th floor
Chicago, IL 60606
Tel: 312.207.1040
Fax: 312.207.1066
plantemoran.com

Section 1. Independent Service Auditor’s Report

To Management of Dovenmuehle Mortgage, Inc.:
Lake Zurich, Illinois

Scope

We have examined Dovenmuehle Mortgage, Inc.’s (DMI) description of its subservicing operation system entitled “Dovenmuehle Mortgage, Inc.’s Description of its Subservicing Operation System Throughout the Period October 1, 2019 to September 30, 2020” (description) and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in “Dovenmuehle Mortgage, Inc. Management’s Assertion” (assertion). The controls and control objectives included in the description are those that management of DMI believes are likely to be relevant to user entities’ internal control over financial reporting, and the description does not include those aspects of the subservicing operation system that are not likely to be relevant to user entities’ internal control over financial reporting.

DMI uses subservice organizations to achieve operating efficiency and to obtain specific expertise. A list of these subservice organizations is provided in the description of the system. The description of the system in Section 3 and the control objectives and related controls listed in Section 4 of this report include only the control objectives and related controls of DMI and exclude the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified in the description can be achieved only if complementary subservice organization controls at the subservice organizations assumed in the design of DMI’s controls are suitably designed and operating effectively, along with related controls at DMI. Our examination did not extend to controls of the subservice organizations and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of DMI's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

In Section 2 of this report, DMI management has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. DMI is responsible for preparing the description and the assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period October 1, 2019 to September 30, 2020. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls involves:

- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion.
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description.
- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.
- evaluating the overall presentation of the description and suitability of the control objectives stated in the description specified by the service organization management in its assertion.

Inherent Limitations

DMI's description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are listed in Section 4 of this report. The scope of our engagement did not include tests to determine whether controls not listed in Section 4 were achieved; accordingly, we express no opinion on the achievement of controls not included in Section 4.

Opinion

In our opinion, in all material respects, based on the criteria described in DMI management's Assertion,

a. the description fairly presents DMI's subservicing operation system for processing user entities' transactions that was designed and implemented throughout the period October 1, 2019 to September 30, 2020.

b. the controls of DMI related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period October 1, 2019 to September 30, 2020 and subservice organizations and user entities applied the complementary controls assumed in the design of DMI's controls throughout the period October 1, 2019 to September 30, 2020.

c. the controls that we tested, which were those necessary to provide reasonable assurance that the control objectives were achieved operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period October 1, 2019 to September 30, 2020 if complementary subservice organization and user entity controls assumed in the design of DMI's controls operated effectively throughout the period October 1, 2019 to September 30, 2020.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4 of this report, is intended solely for the information and use of management of DMI, user entities of DMI's subservicing operation system during some or all of the period October 1, 2019 to September 30, 2020, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than those specified parties.

Plante & Moran, PLLC

December 15, 2020

Dovenmuehle

December 15, 2020

Plante & Moran, PLLC
10 South Riverside Plaza
Chicago, IL 60606

To Service Auditors:

We have prepared the description of Dovenmuehle Mortgage, Inc's (DMI) subservicing operations system entitled, "Dovenmuehle Mortgage, Inc.'s Description of its Subservicing Operations System Throughout the Period October 1, 2019 to September 30, 2020" (description) for user entities of the system during some or all of the period October 1, 2019 to September 30, 2020, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities of the system themselves when assessing the risks of material misstatement of user entities' financial statements.

DMI uses subservice organizations to achieve operating efficiency and to obtain specific expertise. A list of these subservice organizations is provided in the description of the system. The description includes only the control objectives and related controls of DMI and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified in the description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with related controls at the subservice organizations. The description does not extend to controls of the subservice organizations.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of DMI's controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of the user entities.

We confirm, to the best of our knowledge and belief, that:

a. The description fairly presents the subservicing operations system made available to user entities of the system during some or all of the period October 1, 2019 to September 30, 2020 for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:

   i. Presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, if applicable

      1) the types of services provided, including as appropriate, the classes of transactions processed;
      2) the procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system;

3) the information used in the performance of the procedures including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities;

4) how the system captures and addresses significant events and conditions other than transactions;

5) the process used to prepare reports and other information for user entities;

6) services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them;

7) the specified control objectives and controls designed to achieve those objectives including as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the service organization's controls, and control objectives that are specified by law, regulation, or another party; and

8) other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

ii. includes relevant details of changes to the service organization's system during the period covered by the description.

iii. does not omit or distort information relevant to the service organization's system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect of the subservicing operations system that each individual user entity of the system and its auditor may consider important in its own particular environment.

b. The controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period October 1, 2019 to September 30, 2020 to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of DMI's controls throughout the period October 1, 2019 to September 30, 2020. The criteria we used in making this assertion were that:

i. the risks that threaten the achievement of the control objectives stated in the description have been identified by the management of the service organization.

ii. the controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved

iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Very truly yours,

Glen S. Braun

Glen S. Braun, Chief Financial Officer

Section 3. Dovenmuehle Mortgage, Inc.'s Description of its Subservicing Operations System Throughout the Period October 1, 2019 to September 30, 2020

A. Company Overview

Founded in 1844, Dovenmuehle Mortgage, Inc. (DMI or the company) is a mortgage loan subservicing company. Dedicated exclusively to mortgage subservicing, DMI serves over 320 clients and manages over 1.7 million loans with an aggregate principal balance in excess of $417 billion.

DMI subservices loans for its clients on behalf of Fannie Mae, Freddie Mac, the Government National Mortgage Association (GNMA or Ginnie Mae), major private mortgage conduits, portfolio lenders, and private investors. DMI subservices all types of real estate loans, including first and second single-family mortgages, home equity lines of credit, construction loans, and commercial and multi-family mortgages located in 50 states, the District of Columbia, Puerto Rico, and the U.S. territories. These loans are subserviced for portfolio lenders, all secondary market agencies, and over 240 private investors.

DMI employs approximately 1,900 people and performs mortgage subservicing operations at three facilities located in Lake Zurich, IL, North Aurora, IL, and Elgin, IL.

B. Scope of the Report

Scope

This report contains a description of DMI's subservicing operations system for the period from October 1, 2019 to September 30, 2020. The subservicing operations system includes the following services:

- Portfolio Transfer
- New Loan Setup
- Billing and Cashiering
- Special Loan Servicing
- Customer Service and Research
- Escrow Processing and Analysis
- Bank Reconciliations
- Investor Accounting
- Collection Counseling
- Loss Mitigation
- Foreclosure and Bankruptcy Control

Specialized services include:

- Private label subservicing - the program includes the following customer facing media in the name of the client: coupon books, monthly statements, Customer Service Representatives, website, and correspondence
- VIP Private Banking Program, with incoming calls routed directly to a Customer Service Representative and special default reporting to the client
- Remote Inquiry System allowing clients direct access to the DMI loan servicing system for detailed loan inquiry
- Customized management reports prepared in any frequency in all major file formats
- Payoff Alert Service providing a daily electronic report of all requests for verifications of mortgage or payoff statements
- Mortgage servicing website for borrowers to access information on their mortgage loans
- Branch Payment Interface, allowing the client's borrowers to make mortgage payments at the teller window
- General Ledger Interface, providing a daily journal voucher summarizing financial activities
- New Loan Interface, providing custom solution allowing the client to extract data from its loan origination system and place the data on a secured portal allowing DMI to convert the data for upload onto the mortgage processing system

Significant Changes in the System and Controls

There were no significant changes to the internal control environment during the period October 1, 2019 to September 30, 2020.

Subsequent Events

Management is not aware of any relevant events that occurred subsequent to the end of the reporting period through the date of the service auditor's report that would have a significant effect on management's assertion.

C. Subservice Organizations

Management of DMI assumed, in the design of DMI's subservicing operations system that certain controls at subservice organizations are necessary, in combination with controls at DMI, to provide reasonable assurance that DMI's control objectives would be achieved. These complementary subservice organization controls and the related control objectives are described below. Subservice organizations are responsible for implementing such controls.

The following are the subservice organizations used by DMI, services provided by them, and the control objectives that are applicable to the services that they provide:

- **Black Knight Financial Services, Inc. (BKFS) -** Mortgage Servicing Platform (MSP) for computer transaction processing and data storage. MSP is a provider of core processing for financial institutions; transaction processing services; mortgage loan processing and mortgage-related information products; and outsourcing services to financial institutions, retailers, mortgage lenders, and real estate professionals.
- **National General Lender Services, Inc. (National General) -** hazard insurance monitoring and force placement of insurance

- **CoreLogic Solutions, LLC (CoreLogic) -** monitoring and payment of taxes
- **The Bank of New York Mellon Treasury Services (Mellon)** - for lockbox services and payment lockbox processing
- **Iron Mountain Information Management, LLC (Iron Mountain) -** offsite media archival
- **TM Systems Pvt. Ltd (TM Systems) -** offsite data entry
- **NCP Solutions, LLC (NCP Solutions) -** borrower letter generation
- **SunGard Availability Services LP (SunGard) -** disaster recovery site

Complementary Subservice Organization Controls	Related Control Objective
BKFS is responsible for software development and providing software updates relevant to security and processing integrity.	Control Objective 5
National General is responsible for monitoring hazard insurance and communicating force placement of insurance accurately and completely.	Control Objective 9
CoreLogic is responsible for monitoring taxes and communicating payments due accurately and completely.	Control Objective 9
Mellon is responsible for restricting physical access to lockboxes.	Control Objective 2
Mellon is responsible for the accuracy and completeness lockbox activity reporting.	Control Objective 8
Iron Mountain is responsible for implementing physical access controls and environmental protections at the offsite media storage site.	Control Objectives 2, 3, and 13
TM Systems is responsible for the accuracy and completeness of data entry.	Control Objectives 7, 8 and 10
NCP Solutions is responsible for the accuracy completeness of printing and mailing borrower letters.	Control Objectives 8 and 11
SunGard is responsible for implementing logical and physical access controls and environmental protections for the disaster recovery site, monitoring and maintaining systems, and implementing backup and recovery policies and procedures.	Control Objectives 2, 3, 4, 5, and 13

D. Company-Level Internal Controls

Control Environment

Organization and Administration

The organization is structured with clearly defined reporting lines, authorities and responsibilities in the company's organization chart. The organization chart is made available to employees through the company's intranet. Monthly meetings are scheduled with senior vice presidents and department heads to review department operations, performance, and any outstanding issues. Monthly reports provide data for management to assess DMI's performance efficiency, product integrity, and client service standards. Feedback is reviewed with the managers of each department to help ensure continuous operational quality and efficiency. The board of directors includes members that are independent from management and meets at least quarterly to discuss the business operations and monitor internal control operations.

DMI has frequent contact with clients, service providers, external and internal audit, and regulatory bodies. This contact serves as an additional monitoring source for the detection of weaknesses within the system of internal control and service standards.

The Compliance Department monitors regulatory changes through several sources; the primary source is an AllRegs subscription. The Compliance Department also receives updates through MBA, USFN, CounselorLibrary, OCC, the various state agencies by which DMI is regulated, numerous law firms specializing in consumer financial services, and from clients' compliance departments.

Updates to the organization and department responsibilities are reviewed for applicability to subservicing functions. Impacted departments are advised as appropriate.

Personnel Policies and Procedures

DMI's policies and procedures have been established by management and are documented in the DMI Employee Handbook, which is updated promptly as policies or procedures change. The Handbook is distributed to DMI personnel and a current copy is maintained on the company intranet. The Employee Handbook contains disciplinary actions to take against employees whose behaviors deviate from the company's expected standards of conduct. DMI employees are required to sign an acknowledgement during time of hire to indicate that they have read and will comply with the policies as stated in the handbook.

Candidates are evaluated by HR and managers or supervisors as part of the new hire process. Background checks are performed by HR on every employee upon hiring. Background checks cover federal and state violations and financial history. Training is conducted regarding the security of confidential information and compliance with the Federal Gramm-Leach-Bliley Act. All employees are required to sign a confidential information form stating that they will keep all mortgagor information and any other private information strictly confidential.

Annual performance reviews are performed and documented with a checklist that is signed by the employee and the manager. Performance metrics are established for individuals with significant internal control responsibilities, which are evaluated as part of the annual performance reviews.

Risk Assessment

DMI has developed a risk assessment process to identify and manage risks that could affect DMI's ability to provide reliable transaction processing for user entities. The risk assessment process measures business process risk and information system risk.

Internal audit and quality assurance have developed a business risk assessment for each functional area of mortgage subservice processing and conducts its audits based upon the risk level. An ITGC review is performed by the Internal Audit Department on a quarterly basis.

DMI has conducted a risk assessment of its information system including non-electronic information sources and repositories. The assessment identifies the threats to the information system, measures the inherent risk of the threat, assesses the effectiveness of the controls in place to mitigate the risk, and measures the residual risk. The conclusions of the risk assessment are supported by an internal network security assessment which is conducted by an independent third party.

Information and Communication

Each DMI department that performs mortgage subservicing activities has written standards and procedures documents. The documents are made available to employees through the company's internal document management portal.

An Information Security Policy (ISP) exists that documents employee responsibilities for the use of DMI technology, programs, files, unauthorized use of passwords, and the appropriate use of the Internet. Security Awareness Training is provided to employees upon hire to ensure the ISP is effectively communicated to employees.

DMI has a Subservicing Policy Manual that describes the basics of each of the services that DMI will provide for clients and describes the client's responsibilities relating to that service. The Subservicing Policy Manual and DMIConnect Client Administrator Guide inform clients how to report any issues. The Subservicing Policy Manual describes all services and boundaries of the system to clients, and it is provided to clients at the time of boarding. Updates to the manual are provided to clients through DMIConnect. Specific services provided to each client are defined in signed Subservicing Agreements. Security, availability, and confidentiality commitments are communicated to clients via Subservicing Agreements.

DMI websites list contact information. Standard Billing statements contain appropriate DMI contact information for borrowers in the event of questions or concerns.

All changes are evaluated for whether communication is required to notify affected internal and/or external users. When applicable, affected users are notified via email.

Monitoring Activities

Quality Assurance

DMI's Quality Assurance Department is responsible for auditing the operational compliance of all servicing departments within Dovenmuehle. The department is independent of operational management and reports directly to the Board of Directors. The reviews performed by Quality Assurance satisfy Housing and Urban Development (HUD) and agency quality assurance requirements.

On an annual basis the Quality Assurance Plan is developed and lists all audits that are to be completed in the year. The Plan includes reviews that are performed monthly, quarterly, semi-annually, and annually and is based on the Office of the Comptroller of the Currency's ("OCC") sampling methodology for compliance testing. It was designed and implemented by DMI in support of its commitment to ethical and compliant subservicing.

It consists of function-driven mortgage loan subservicing reviews that are performed by independent, knowledgeable personnel at DMI who have no direct mortgage servicing responsibilities.

As Quality Assurance audits are completed, a report is created that includes any findings and management responses to those findings. Additionally, reports contain objective trending information that assists the reader in understanding how an area has performed over time. Upon completion, each report is presented to Operational Management and on a quarterly basis the reports are presented to DMI's Board of Directors.

Internal Audit

DMI has an Internal Audit Department that plays a key role in monitoring the control environment and assessing risk. The Internal Audit Department conducts a variety of compliance, operational, and information technology audits. Internal Audit utilizes a risk-based audit plan to determine the department's priorities. The related risk assessment is undertaken at least annually and includes the input of senior management and the Board of Directors. Audits included in the audit plan are rotated on a 3-year rotation schedule depending on their risk rating. High risk areas are tested annually, while lower risk areas may be tested less frequently.

For each audit engagement, the auditor must develop and document a plan for each engagement, including the engagement's objectives, scope, timing, and resource allocations. The Director of Internal Audit oversees each audit via an Audit Checklist where internal auditors are given audit steps with accompanying completion dates. The Director of Internal Audit must sign off on each of the steps completed in the audit checklist starting at planning the audit all the way up until the audit report is finalized.

The results of the audits are reviewed by management. Management resolves any issues identified during the audit process and implements recommended improvements. On a quarterly basis, the Director of Internal Audit reports to the Board of Directors and the Audit Committee to discuss audit results and the status of the Internal Audit Department.

Members of DMI's internal audit function performed tests of controls for the following control objectives:

- Controls provide reasonable assurance that the structure of the organization provides for management oversight and separation of duties and established policies and procedures with regards to information technology and performance of key business processes are communicated and adhered to.
- Controls provide reasonable assurance that physical access to computer equipment, storage media, program documentation, and hard copy of computer data containing customer information is limited to authorized personnel.
- Controls provide reasonable assurance that logical access to applications and data is limited to authorized individuals.
- Controls provide reasonable assurance that systems are monitored for performance, maintenance, capacity and security issues; that system software is kept at current release and patch levels; and that change requests to MSP are properly authorized.
- Controls provide reasonable assurance that loans are properly set up in the system and that all loan parameters and beginning balances agree to the information and balances supplied by the client.
- Controls provide reasonable assurance that loan payments are received and processed accurately and completely, and that special loan servicing is accurate, complete, and timely.

- Controls provide reasonable assurance that escrow accounts are processed properly, that account balances are correct, that escrow disbursements are timely, and that interest payments and excess amounts are properly processed.
- Controls provide reasonable assurance that account reconciliations occur on a timely basis, are complete and accurate, and that all reconciling items are resolved in a timely manner.
- Controls provide reasonable assurance that processing of delinquent accounts is in accordance with applicable servicing guidelines; that delinquent accounts undergo loss mitigation procedures prior to being referred for foreclosure; and that applicable federal, state, and client guidelines are followed for accounts placed in foreclosure.
- Controls provide reasonable assurance that client concerns are addressed and resolved in a timely manner and according to client requirements.

The tests performed by members of the internal audit function included inquiry of relevant parties who performed the control activities, observation of the control being performed at different times during the examination period, and inspection of the documentation for a sample of transactions.

Control Activities

Control activities are deployed through policy and procedure documents. Senior management is accountable for control activities. Segregation of duties are implemented in the administration of logical access and change management functions, which are considered to be significant and high risk functions. The risk assessment utilizes a combination of preventative, detective, automatic, and manual controls to manage risks.

E. Components of the Subservicing Operations System

Summary of the Subservicing Operations System

DMI hosts borrower websites that allow borrowers to access basic loan information such as payment due date, loan history, escrow information, and 1098 forms. The website enables the borrower to make individual mortgage payments online with a one-time drafting option, or to enroll for a recurring monthly draft, all without having to call Customer Service. Certain loans are not eligible for online drafting including loans with bad check stops, processing stops or foreclosure stops. The website also provides up to 24 months of detailed account activity, year-to-date balances and images of the 1098 statement and the escrow analysis statement for the prior year.

Clients have the option to choose between a Gold website or a Silver website. Gold websites allow clients to request additional customizations, including the option of allowing their borrowers to authenticate to the borrower website via their bank account login information (“single-sign-on” or SSO). Gold websites can be customized with the client’s name, logo and graphics to provide the same customer experience as the client’s home website.

Infrastructure

DMI's internal network infrastructure runs primarily on Microsoft Windows servers using a wide area network. Employees are able to access internal applications such as DMI's imagining system and internal procedure portals through their desktop on company-supplied computers or through a SonicWall Access Gateway.

DMI's primary data center is located within its Lake Zurich, IL facility. It is located on the third floor of the building and is secured by a badge reader and cypher lock. Only authorized individuals have access to enter the data center. The data center is monitored by CCTV. Additionally, it is monitored for temperature, smoke, water, humidity with alerts being sent to relevant IT staff. DMI has a backup data center located in its North Aurora, IL facility with controls similar to the primary data center.

Data communications between DMI's three offices are encrypted using TLS 1.2/AES 256-bit encryption to protect data and intra-company communications.

Software

The primary system of record utilized by DMI for the servicing of loans is MSP. MSP runs on Black Knight's mainframe server hosted at their Virginia data center. DMI connects to MSP via a dedicated circuit to the MSP Mainframe in order to maintain a secure connection.

DMI provides clients with online access to corporate and loan level documents through the DMIConnect system. Items such as policies, procedures, due diligence documents, servicing documents, newsletters, and client announcements are accessible. This system provides clients access to other DMI products such as Servicing360, RIS, WebDirect, and TellerView. Access to DMIConnect is managed by client's designated Administrators while access to some of the specialized products within DMIConnect, such as RIS, are managed by DMI.

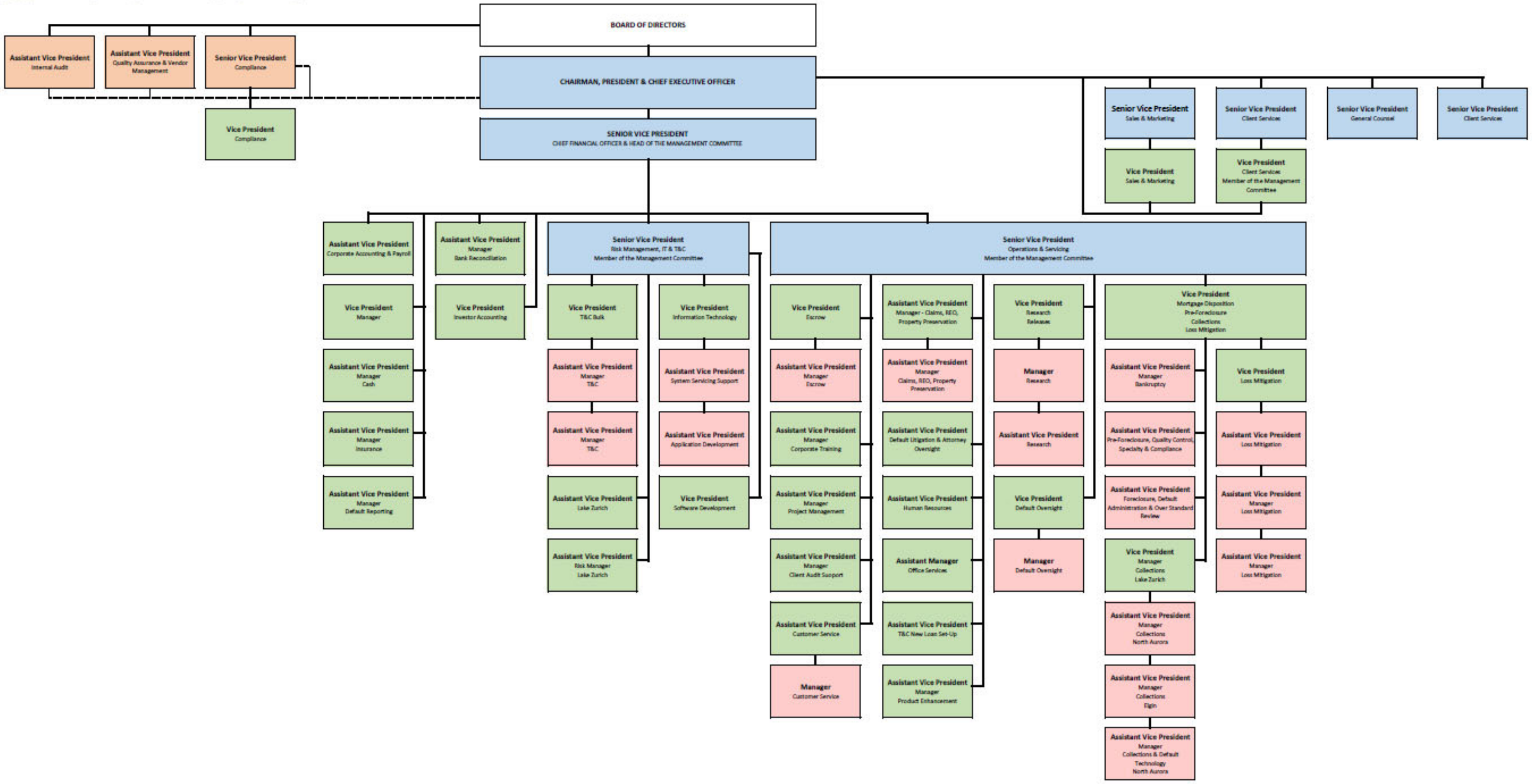
DMI offers clients a choice of two borrower-facing websites that will provide borrowers with detailed payment history, escrow account activity, year-to-date balances, and online payment capabilities. These websites are created by DMI developers based on client requirements and are stored on servers located at DMI's Lake Zurich facility. Backup servers for the borrower websites are located at a SunGard facility in Arizona.

People

The DMI organizational chart depicts the departments responsible for providing services for clients. Job descriptions are documented and specify the roles and responsibilities of internal users.

Senior management of DMI plays a significant role in ensuring the control environment is functioning properly. Daily meetings are held with DMI senior managers. These meetings cover the departments' processing activities, workforce productivity, upcoming events, current projects, and projected staffing needs. Where available, departments are required to provide summary reports tracking activities. Strategies for typical contingencies and problem resolution are also discussed.

Dovenmuehle


BOARD OF DIRECTORS
CHAIRMAN, PRESIDENT & CHIEF EXECUTIVE OFFICER
SENIOR VICE PRESIDENT CHIEF FINANCIAL OFFICER & HEAD OF THE MANAGEMENT COMMITTEE
Assistant Vice President Internal Audit
Assistant Vice President Quality Assurance & Vendor Management
Senior Vice President Compliance
Vice President Compliance
Senior Vice President Sales & Marketing
Vice President Sales & Marketing
Senior Vice President Client Services
Vice President Client Services Member of the Management Committee
Senior Vice President General Counsel
Senior Vice President Client Services
Assistant Vice President Corporate Accounting & Payroll
Vice President Manager
Assistant Vice President Manager Cash
Assistant Vice President Manager Insurance
Assistant Vice President Manager Default Reporting
Assistant Vice President Manager Bank Reconciliation
Vice President Investor Accounting
Senior Vice President Risk Management, IT & T&C Member of the Management Committee
Vice President T&C Bulk
Assistant Vice President Manager T&C
Assistant Vice President Manager T&C
Assistant Vice President Lake Zurich
Assistant Vice President Risk Manager Lake Zurich
Vice President Information Technology
Assistant Vice President System Servicing Support
Assistant Vice President Application Development
Vice President Software Development
Senior Vice President Operations & Servicing Member of the Management Committee
Vice President Escrow
Assistant Vice President Manager Escrow
Assistant Vice President Manager Corporate Training
Assistant Vice President Manager Project Management
Assistant Vice President Manager Client Audit Support
Assistant Vice President Customer Service
Manager Customer Service
Assistant Vice President Manager - Claims, REO, Property Preservation
Assistant Vice President Manager Claims, REO, Property Preservation
Assistant Vice President Default Litigation & Attorney Oversight
Assistant Vice President Human Resources
Assistant Manager Office Services
Assistant Vice President T&C New Loan Set-Up
Assistant Vice President Manager Product Enhancement
Vice President Research Releases
Manager Research
Assistant Vice President Research
Vice President Default Oversight
Manager Default Oversight
Vice President Mortgage Disposition Pre-Foreclosure Collections Loss Mitigation
Assistant Vice President Manager Bankruptcy
Assistant Vice President Pre-Foreclosure, Quality Control, Specialty & Compliance
Assistant Vice President Foreclosure, Default Administration & Over Standard Review
Vice President Manager Collections Lake Zurich
Assistant Vice President Manager Collections North Aurora
Assistant Vice President Manager Collections Elgin
Assistant Vice President Manager Collections & Default Technology North Aurora
Vice President Loss Mitigation
Assistant Vice President Loss Mitigation
Assistant Vice President Manager Loss Mitigation
Assistant Vice President Manager Loss Mitigation

Data

All DMI data is identified and classified into the following categories:

- Borrower
- Business Partner/Vendor
- Client
- Employee
- Financial
- General

The main system of record for borrower data is MSP. This system houses thousands of borrower mortgage-related datapoints and is accessible by DMI employees and clients. Access to this system is managed by DMI's Servicing Systems Support Department.

Output reports from the MSP system are stored initially as text/CSV files and, based on the type of report, are imported into DMI's data warehouse, and parsed by client to be distributed. Reports are stored in DMI's file servers at the Lake Zurich facility. When transmitting reporting to clients, files are placed on the client's segment of the SFTP Server for retrieval.

Other forms of DMI data is housed locally at DMI's primary data center in Lake Zurich. Access to this data is role based and is managed, primarily, by Active Directory. Users are only granted access to the data required to perform their job responsibilities.

Procedures

Physical Security

DMI has offices in three locations, Lake Zurich, Illinois, North Aurora, Illinois, and Elgin, Illinois. Access to all facilities is controlled by an electronic key card system. Access cards for the Lake Zurich building are maintained by building security. Access cards and access levels are granted based upon an Access Card Request form that is submitted by DMI. DMI administers the badge system in Elgin and North Aurora. Administrative access to the badge systems at Elgin and North Aurora is limited to HR, Executive Support/Business Continuity, and the Facilities Manager. The HR department conducts a quarterly review of access levels to the building and suite for all three office locations.

All visitors to the Lake Zurich facility must sign in at the security desk and present their identification. Visitors must be escorted by a DMI employee. Visitor badges are provided to Lake Zurich visitors. All electronic key cards for visitors are accounted for each day by the building security. Any missing cards are deactivated each night. Similarly, visitors to the North Aurora and Elgin facilities must sign in and be escorted by a DMI employee. The Lake Zurich building has a burglar alarm that is monitored 24/7 by the building's security agency. The Elgin and North Aurora offices have burglar alarms that are monitored 24/7 by TYCO. All three office buildings have video cameras monitoring all entry points.

The Cashiering Department is located in an inconspicuous, secure location at the Lake Zurich office. Access to the Cashiering Department is controlled by an electronic badge system and is limited to authorized employees. All other employees or visitors are escorted when within the Cashiering Department.

DMI utilizes an employee Termination Notice/Checklist form to manage the process of terminating an employee. The form includes collecting the electronic swipe cards for all locations. The Human Resource Department notifies Lake Zurich building security of all terminations at the Lake Zurich location and the Managers in Elgin and North Aurora of all terminations at the Elgin and North Aurora locations within one business day.

Application Development and Change Management

DMI uses the Black Knight Financial Services' Mortgage Servicing Platform (MSP) application. DMI does not have the ability to perform any changes to the MSP application. DMI can request changes be made to the MSP systems via an online request process. Authorization to request changes to MSP is limited to the MSP group. MSP informs DMI of all changes made (either requested by DMI or other customers) and new versions of the software via client update advisories. DMI tests the updates from MSP as necessary before installing updates.

Change management procedures are in place for the servers, firewall, and virtual private network (VPN) concentrator. Changes can only be performed by authorized members of the Information Technology Department (IT Department). DMI has implemented a software development life cycle (SDLC) policy which prescribes the authorization, development, UAT, and the final push to production. The SDLC policy is reviewed on an annual basis. All changes must be authorized by a Team Lead or Manager prior to development. All changes must be tested by development staff, project management, or client based on the request type. User Acceptance Testing (UAT) is completed as needed. All changes must be approved by the Development Manager or Director of IT after testing, prior to migration into production.

Environmental Protections

DMI's internal network architecture is protected with environmental control mechanisms such as fire extinguishers, temperature controls, and uninterruptible power supplies.

The Lake Zurich, North Aurora, and Elgin facilities are monitored 24/7 by a fire detection system. The systems are monitored by the respective local fire departments. Fire extinguishers are placed throughout the Lake Zurich, North Aurora, and Elgin office facilities according to local fire code. The Lake Zurich and North Aurora data centers are equipped with smoke detectors and electrically rated fire extinguishers. All fire extinguishers are serviced at least annually.

The data centers in Lake Zurich and North Aurora are temperature controlled via dedicated HVAC systems. Temperature sensors are in place and configured to send alerts to IT personnel when the temperature rises above a certain threshold. Servers are protected from power surges, brownouts, and failures through the use of an uninterruptible power supply (UPS) unit. The UPS maintains server power and provides for a controlled shutdown of the servers. UPS units are scheduled to perform self-tests every two weeks.

The data center located in Lake Zurich is located on the third floor of the building to protect against flooding. The data center has a raised floor and equipment is stored on equipment racks. Equipment is stored on equipment racks at the backup data center in North Aurora.

Data Backup and Recovery

DMI runs differential backups of its server environment daily. To monitor for the completion of backup jobs, alerts are sent to the IT Department when backup jobs are not completed successfully. Full backups are performed weekly and rotated off-site to a records management company. Data backup tape restores are performed by the IT System Administrators quarterly.

All production data resides at DMI locations. Lake Zurich is the primary data center location. The backup data center is located in North Aurora. DMI maintains a Business Continuity Plan. The Business Continuity Plan identifies the North Aurora location as a warm backup site for the Lake Zurich location, and vice versa. The Plan also identifies SunGard as DMI's vendor for secondary disaster recovery facility. Continuous data replication is performed on a 24/7 basis to facilitate recovery of critical systems within hours of declaring a disaster. In addition, DMI also has an agreement with its disaster recovery provider that allows DMI to perform customer service and processing duties at this secondary disaster recovery facility. The site is equipped with telephones and computers sufficient to continue the daily efforts relative to MSP connectivity as well as independent production. An annual disaster recovery test is performed at the secondary disaster recovery facility and DMI reviews the test results. Testing includes the ability to set up and restore network servers and workstations, establish connectivity to MSP, process MSP transactions, and establish telecommunications using DMI's toll-free numbers at the secondary disaster recovery site.

Authentication

Logical access to DMI applications and data is limited to properly authorized employees and authorized computer equipment. The logical access is divided into three areas: the Local Area Network (LAN), Windows Active Directory/Application level security, and the MSP application.

Logical access is controlled via user IDs and passwords. The LAN password policy requires passwords to be a minimum of eight characters, to expire every 45 days, and to meet complexity requirements. The last 24 passwords cannot be reused. After five incorrect password attempts, the account is locked out for 15 minutes. A screen saver is enabled after 10 minutes of inactivity. The MSP password policy requires a minimum of eight alphanumeric characters, must meet complexity requirements and expire at least every 90 days. The account sessions time out after 20 minutes of inactivity.

Access to the network and data level access is limited to authorized employees. Network and data access for new employees and changes to existing employee access levels are granted via a security change request. The change request is submitted by staff to the department manager(s) for approval. Once the security change request is approved, it will be submitted to the Information Technology Department (IT Department) via the helpdesk. The helpdesk is responsible for processing the approved access to systems.

VPN access and web Client Portal access are granted on a limited basis to certain employees and are approved through the security request form process. Secured token and 2048 bit connection is required for VPN access. VPN sessions are timed out after 15 minutes of inactivity.

IT sends Active Directory and MSP user lists to department managers for review on a quarterly basis. Department managers review the listings to ensure access levels are appropriate and only authorized users have access.

Network administrative access level is limited to members of the Systems Department who require that level of access to perform their job duties. Administrator level access to the MSP system is limited to only those authorized individuals requiring that level of access to perform their job duties.

Clients can access their reports and upload new files via a Client Portal web connection. Three emails are sent out to the client by IT Helpdesk when new accounts are created. One includes the RIS Client Manual, the second consists of the username, and the third indicates the end-user's password.

Clients are granted remote access through a web interface based on an authenticated ID upon authorization from the client. User accounts for client access to the MSP system are restricted from accessing loan information of other clients. The web interface is secured with TLS encryption and passwords must be complex with a minimum of eight characters. In addition, client's IP address ranges are hardcoded in the firewall rule set to explicitly allow traffic only from preauthorized sources.

The Systems Department is notified of employee terminations at the time of termination through the help desk system and logical access is revoked by Helpdesk within two business days. After three days of unexplained absence, employees are terminated. For employees resigning without notice, the LAN and MSP user accounts are deleted within five business days of their last day worked.

Vendor Management

DMI has a vendor management program in place to identify critical vendors and monitor vendor service level performance. DMI enters into a service contract with all key third-party vendors and identifies all vendors with access to confidential customer information. The Legal Department and the related Operational Management completes the Vendor Contract Review Checklist to ensure each vendor contract includes a confidentiality agreement, business resumption and contingency plans, the right to audit performance and GLBA compliance. The CFO ranks vendors by criticality and reviews vendors on a rotational basis. Monitoring is performed on an annual basis. This monitoring includes the completion of a vendor scorecard, obtaining proof of liability insurance, checklists and templates for financial analysis, a vendor assessment and supplemental foreign-based assessment if applicable, contract review, SSAE 18 or equivalent document review, and business continuity plan review. Internal Audit reviews vendor SOC or ITGC reports to verify there are no significant deviations related to services being provided to DMI and the CFO reviews the financial statements of the vendor to determine whether the vendor is solvent and evaluates vendor overall performance against the objectives specified in service level agreements.

Incident Management

As documented within the Information Security Policy (ISP) , the IT Steering Committee is responsible for the system's security, confidentiality, and availability commitments. The Director of IT oversees the IT Steering Committee. The IT Steering Committee is responsible for ensuring potential events and incidents are acted on in accordance with the Incident Response Policy (IRP). All security, availability, or confidentiality events and incidents are discussed as part of the monthly IT Steering Committee meetings. The Incident Response Team and Security Administrator investigates and tracks identified incidents until resolution and notifies affected internal and/or external users.

Information Systems Infrastructure

The DMI network is designed as a logical three-tiered, screened subnet protected by a firewall which controls and limits the type of network traffic allowed in and out of the network. Customer access to the DMI systems is through a web-based Client Portal with SSL and IP filtering. Employee VPN is performed through an SSL VPN appliance utilizing multi-factor authentication.

DMI is a remote user of the MSP System and is connected through a dedicated leased line using 3270 Software to access the system at the desktop.

Software and Network Monitoring

All file servers, routers and network devices are monitored by the IT Network Security Team for system events. Firewall logs are retained for at least 60 days to provide for forensic investigation if needed. An Intrusion Detection System (IDS) and Intrusion Protection System (IPS) is in place to detect suspicious activity. It is configured to notify the IT Department of suspicious activities. Alerts are investigated by the IT Department and resolution is tracked within the ticketing system.

The PRTG Network Monitoring software is configured to alert the Systems Department of the occurrence of certain events or performance thresholds. Resolution and uptime status are tracked within the PRTG monitoring software dashboard. The network monitoring software also monitors uptime, bandwidth, and system capacity. The IT Department reviews uptime, bandwidth, and system capacity on a daily basis.

Alerted issues that require follow-up and all anomalies from the reviews are documented in the help desk ticket system. Anomalies must be approved by the VP of Systems for IT related anomalies, and the MSP Administrator for MSP related anomalies.

Servers and workstations running the Microsoft operating system are updated via the Windows Software Update Services (WSUS). Updates are approved by the Systems Department manager and are applied in “stealth” mode preventing users from interfering with the update process.

Antivirus software is installed on all servers and workstations at DMI. A server is configured as an antivirus management console and management server. That server checks the antivirus vendor’s website periodically throughout the day for updates and pushes the updates to the other servers and workstations as they are received. The software scans machines for viruses in real-time.

The MSP mortgage processing system produces daily error reports and edits. These reports are published to DMI's system and reviewed by department managers daily.

Portfolio Transfer and New Loan Setup

Portfolio transfers occur via file-to-file transfers. The file-to-file loan transfer procedures are documented in New Loan Setup Guide documents. The documents contain detailed procedures covering the loan setup, conversion, and boarding processes.

The file-to-file process is used to convert existing portfolios and newly originated loans. Existing portfolio conversions are also referred to as bulk/mini-bulk, and newly originated loans are referred to as flow loans. For flow loans, clients submit data files through the secured client specific web Portal. File-to-file loans are boarded using the MSP Electronic Loan Interface (ELI) or the New Loan Interface (NLI). ELI is a MSP supported data mapping application that supports many common file types and can be used for bulk or flow loans. Data loaded into ELI is received from clients in pre-mapped spreadsheets. When new file-to-file loans are received by DMI, an automatic email is sent to the Electronic Loan Interface (ELI) Proxy mailbox. The Coordinators check the inbox several times per day and move the e-mails from the inbox to the client's appropriate folder as the loans are boarded. For ELI, the customer is responsible for reviewing the accuracy and completeness of data loaded into the live environment. Data loaded into NLI is received from clients and requires data mapping prior to loading. NLI is programmed by DMI to convert client data files to a transaction file that is accepted by MSP. New NLI implementations are subject to the planning, programming, testing, and final conversion phases. For NLI, data is loaded into a test environment by Data Mappers and reviewed by New Loan Setup Auditors for data mapping, file integrity, cash balances, interest rate parameters and total loan count. The customer must approve the data mapping prior to loading into the live environment.

A New Loan Setup Auditor reconciles live loans against actual loan documents for 100% of all loans added during the first 90 days after the go-live date for both ELI and NLI loan setups. All conversion issues identified in each stage of the process are reported to the client so that they can be addressed and corrected.

The MSP mortgage processing system contains systematic checks to prevent new loans from going "live" if key information is missing, is illogical, or if the loan does not amortize properly. DMI's Flow Tracker Software is used to monitor the status of file-to-file conversions.

It is common that escrow data, related to tax and insurance, cannot be converted within the file-to-file loan setup process, therefore escrow records are set up manually. Setup reports are run daily by New Loan Setup staff from the New Loan Flow Tracking system, which monitors loans until setup is completed. These reports compile a list of loans that have been received and need escrow record setup. When the report is complete an email is sent to the offsite data entry provider as notification that the reports are available for processing. The offsite data entry provider is responsible for setting up the escrow information for each loan. After the information is setup the offsite data entry provider audits each loan for accuracy. A monthly report for missing data is also compiled using MSP Passport System. The reports are saved to a monthly folder for the offsite data entry provider to retrieve and correct any exception.

Billing and Cashiering

Borrowers are sent payment coupon books or monthly billing statements depending upon each client's preference. Monthly billing statements can include customized marketing messages or "statement stuffers."

The Print Vendor Liaison sends daily statements or weekly coupon book requests to a vendor for printing and mailing. The print vendor liaison group monitors the accuracy and timeliness of the printing of statements and coupon books generated by the print vendor on a daily basis. DMI monitors the accuracy of statements and coupon samples using the print vendor's secure online portal. Daily and weekly reconciliations are performed by the Print Vendor Liaison to ensure payment coupon books and billing statements are printed and mailed out timely.

Mortgage payments can be processed by one of four lockbox services located throughout the United States; sent directly to DMI; by direct debiting of the borrower's bank account; by website one-time drafting; by Bill Payment Services; by ACI Speedpay; or by payments made at the client's branches and forwarded to DMI. All funds are deposited daily into a central payment clearing account and then transferred, as appropriate, into client or agency custodial accounts.

Lockbox checks are opened in a secure room that is controlled via key pad code. Access is limited to Cashiering personnel. Checks are then transferred to the Cashiering Department for processing. At the end of each day, all checks are locked in the Cashiering Department in a fire proof safe which is restricted to authorized Cashiering Department personnel. Lockbox checks are imaged and processed using the MaxPay application. The loan number and amount are keyed by Cashiering employees during the imaging process. After imaging, payments are batched and posted to MSP. Payments that are rejected by the system are automatically sent to the appropriate rejection queue for review. At the end of each day, payments that can be posted to MSP are encoded and endorsed for deposit into the bank. Quality Control employees compare the check amount with the amount encoded to ensure payments are posted accurately. Payments that remain unresolved are populated on the Payments Pulled Report, investigated, and resolution is documented in the MSP loan history.

ACH payments are batched and auto-posted to MSP. Payments that do not post automatically are sent to the suspense account. On a weekly basis, Aged Suspense Reports are sent to the departments affected for review. The online system used by borrowers to make payments is secured via HTTPS encryption.

On a daily basis, the total amount of borrower cash receipts processed are reconciled to the batch totals posted to the system.

Special Loan Servicing

Special loans, defined as loans that do not have a fixed interest rate, have scheduled changes (e.g., balloon notifications/resets, interest only to principal and interest (P&I) conversion, step rate notifications, subsidy/buy-down administration, construction rollover, HELOC open-end process, etc.) per the note, and loans modified upon request (e.g., interest rate & term modifications, recasts, name changes, partial releases, assumptions, trust transfers, successor in interest, subordinations, etc.) which are serviced according to information provided by the client during the loan setup process, the investor's guidelines, and all applicable regulatory requirements.

Interest rate indices are checked daily and the MSP system is updated when rate changes occur. Adjustable Rate Mortgage (ARM) rate adjustments are verified daily by the Special Loans Department in accordance with the proper index, look-back method, remaining term and rounding. DMI is responsible for creating and mailing to the borrowers an initial and a subsequent rate adjustment notification letter. A hard copy of the actual interest rate table that the rate change was based upon is scanned into DMI's system and retained indefinitely.

Date of rate change and index lead days are maintained within MSP for ARM loans. A daily report is run to identify loans requiring rate changes. The Special Loans Supervisor reviews daily reports and verifies that rate changes were calculated accurately by the system. When ARM loans require first-time rate changes, indices are reviewed by the Special Loans Department against loan terms, calculated, and updated in MSP.

System tapes used to prepare notification letters are generated automatically every five business days. Each week the total number of loans adjusted is compared to the total number of letters sent. If the numbers do not agree, the loans that have not had a letter generated are investigated and a manual notification letter is prepared and sent. If a tape is not released for 5 business days, the system will automatically release the tape to the vendor for printing.

DMI offers a data verification service for transferred adjustable rate loans. DMI will:

- Compile an inventory of the loan note for loans that have not gone through the first rate adjustment
- Perform quality control of the exception reports
- Provide system maintenance as necessary
- Report exceptions to the client
- Issue refund checks (if necessary)

Key ARM data elements are compared against the ARM Note for all ARM loans setup on the system, if a copy of the Note is provided by the client. This review is completed prior to the anniversary date of the first rate adjustment. Auditing of ARM loans in existing portfolio transfers is performed based upon parameters mutually agreed-upon by DMI and the client. Errors identified in the auditing process are resolved in a timely basis.

Customer Service and Research

The DMI Call Center is open from 7:00 a.m. to 7:00 p.m., U.S. Central Time, Monday through Friday. Call Center Representatives answer private label calls using the client's name and approved greeting. DMI monitors Call Center service levels for call answer rate, abandonment rate, and average speed of answer on a daily basis. Call Center performance is reported to Senior Management on a monthly basis. Call center performance is evaluated by monitoring eight to ten calls per representative each month by the Customer Service Quality Control Team.

DMI utilizes an automated answering system to allow borrower access to loan information. A standard Interactive Voice Response call path and structure exists which allows borrowers to exit the system at any time to speak directly with a Customer Service Representative. DMI provides toll-free numbers for use by all borrowers. For VIP borrowers, calls are answered directly by a Customer Service Representative with a specialized team, in addition to other specialty services provided.

Inquiries that cannot be answered immediately are set up as a task in the DMI system and forwarded to the appropriate department. The caller is informed of the estimated time that it will take to respond to their inquiry. DMI has established a listing of over 1,100 common requests and has assigned an expected time to complete to each task. If a specific task cannot be completed within the original time estimate, the borrower is notified and provided with a new expected completion date. On a daily basis, the task reports are emailed to Managers, Assistant Managers, and Supervisors to ensure tasks are completed in a timely manner and according to expected completion dates assigned in the system.

DMI accepts written customer inquiries through either the U.S. Post Office, facsimile, Secured Website, or Internet email. When a written request for information or error resolution is submitted to DMI, an acknowledgement letter must be sent to the borrower. All written inquiries receive an acknowledgement letter in accordance with the Real Estate Settlement and Procedures Act (RESPA).

DMI is responsible for generating the payoff letter. Loan payoff processing by the Release Department includes a calculation and check of interest due and the generation of a payoff letter that lists principal, interest, and any escrowed amounts due. DMI has a formal review process in place to determine whether positive escrow balances are refunded to borrowers.

Escrow Processing

If the loan is escrowed and as applicable, DMI is responsible for the payment of all property taxes, hazard insurance premiums, FHA mortgage insurance premiums, private mortgage insurance premiums, flood insurance premiums, forced placed fire/flood insurance, and for controlling the disbursement of funds for hazard insurance claims. Policies are audited annually to verify that limits are adequate and that the carrier has an A.M. Best credit rating acceptable to the agency or investor.

DMI uses a third-party tax service to disburse appropriate payments from the mortgagors escrow account, remit the funds to the county, update tax escrow records, and for non-escrowed accounts monitor county records, to ensure the taxes are paid timely.

A Delinquent Loans with Overage report is reviewed on a daily basis by an Escrow Analysis Representative to ensure loans with errors and stops are resolved. The Escrow Analysis Representative's review of daily Delinquent Loans with Overage reports is reported upwards to the Escrow Manager on a monthly basis, using the Analysis Work Schedule.

DMI performs an annual analysis of each escrowed loan to ensure sufficient funds have been deposited into the escrow account and future escrow payments are at the appropriate amount to cover projected tax and insurance payments. A trial analysis is run by the escrow department prior to the scheduled annual analysis, and exception reports are reviewed and corrected. The process is repeated until all errors are resolved. The trial analysis includes verification that all tax accounts are paid and current. The annual escrow analysis includes calculations to determine if there is excess escrow. The annual escrow analysis is performed for each loan after the final property tax bill for that year has been paid. Following the analysis, the borrower receives a new coupon book or billing statement detailing any changes to the monthly mortgage payment. Excess escrow funds are refunded in compliance with RESPA. The system will automatically generate a refund check to the borrower for any excess escrow above $50. The Escrow Analysis Representative's review of daily Delinquent Loans with Overage reports is reported upwards to the Escrow Manager on a monthly basis, using the Analysis Work Schedule. Loans paid in full are automatically analyzed for remaining escrow balances. Positive balances in escrow are automatically refunded to borrowers.

The check printer and check stock are stored in a room that is secured via physical key lock. Authorized DMI check signers are limited to the CFO and Senior Vice Presidents.

DMI's legal department monitors individual state requirements for interest on escrow and adjusts system parameters as needed. Interest earnings are credited to the borrower's account in accordance with state requirements.

All non-escrowed loans are reviewed by the escrow department annually to make sure tax payments are current. DMI communicates with the borrower on all loans with delinquent taxes. If the borrower does not bring the taxes current, DMI will pay the tax and establish an escrow for the loan. DMI also monitors all escrowed and non-escrowed loans for insurance coverage. If an updated policy is not received, DMI will force place hazard insurance effective 56 business days after the policy expiration date, retroactive to the expiration date. Flood insurance will be placed 45 business days after expiration.

Investor Accounting, Bank Reconciliations, and Information Access Options

DMI's Investor Accounting Department reports, remits, and prepares reconciliations for all mortgage agencies, multiple private investors, and various state housing agencies. All types of investor remittance methods are serviced, including "scheduled/scheduled", "scheduled/actual", and "actual/actual." DMI has achieved a Tier 1 Servicer Performance rating by GNMA.

Account reconciliation and reporting are performed monthly for custodial bank accounts in compliance with the minimum servicing standards set forth in the Uniform Single Attestation Program by the Mortgage Bankers Association of America (USAP). The Bank Reconciliation Department utilizes DMI's Bank Account Manager application to track the status of all custodial bank accounts requiring reconciliation. The AVP of Bank Reconciliations monitors account reconciliations for completeness throughout the month. Reconciliations are performed by the Bank Reconciliation Department and are approved by the department management team (supervisor, assistant manager or manager) with the following exceptions: Federal National Mortgage Association (FNMA), Mortgage Backed Security (MBS) P&I, Federal Home Loan Mortgage Corporation (FHLMC) P&I, and BNY Mellon P&I reconciliations are performed by the Investor Accounting

Department and are approved by that department management team (supervisor, assistant manager, or manager). Bank account reconciliations will be completed on or before the next bank statement cutoff date with the following exceptions: GNMA bank account reconciliations will be completed on or before the 30th calendar day from the previous issuer cutoff date per GNMA guidelines and FHLMC bank account reconciliations will be completed on or before the 45th calendar day from the previous cutoff date per FHLMC guidelines.

A monthly package consisting of a client's reconciliation copies and a Reconciliation Account List report will be sent to the client by first class mail, secure email with a single PDF file, or posted to the client's Dovenmuehle FTP Output folder on or before 45 calendar days from the previous investor or bank statement cutoff, whichever is later. If the 45th calendar day falls on a day Dovenmuehle is closed for business then the deadline will be extended to the next business day.

DMI's standard is to clear reconciling items within 30 days. Should an item remain outstanding over 90 days, it is reviewed by senior management. Appropriate documentation will accompany the reconciliation for those items requiring client research or client clearing.

DMI provides clients with standard reports and optional reports based on client requirements. Custom ad-hoc reports and electronic data extracts can be prepared individually for clients. General ledger journal activity is available in electronic format for daily download. Upon request, DMI will create a custom general ledger interface. All electronic information is available through a secured client specific web Portal by 9 a.m. Central Time each business day. Custom requests can be provided earlier.

DMI's Remote Inquiry System provides client access to the mortgage subservicing system via the secured client specific web Portal. The Remote Inquiry System is available Monday through Friday, from 7:00 a.m. to 9:30 p.m. and Saturdays from 7:00 a.m. to 5:00 p.m. Central Time.

DMI provides borrower access to loan history and approximately 40 loan level fields of data via the Internet. DMI can develop a private label client website linked directly to the DMI website for borrower access.

Collections, Loss Mitigation, and Foreclosure

The Collections Department monitors and follows the specific collections guidelines as set forth by clients and agencies including FHA, Veterans Administration (VA), FNMA, FHLMC, and RHS. DMI has developed a 150-day collection timetable that is used by the Collections Department to provide guidelines for collection activities. Collection Timetables are published in the Subservicing Policy Manual. The Collections Department is open until 10 p.m. Central Time on weekdays and 4:00 p.m. Central Time on Saturday to provide the ability for frequent contact with borrowers.

Collection processing follows the guidelines established in the Collections Policy and Procedures to notify borrowers of delinquency. Loans in collection are automatically assigned to Dialer Campaigns based on loan type (configured during loan setup). Dialer Campaigns are configured to comply with the requirements of the Collections Policy and Procedures. Each day Dialer Campaigns are scheduled for calling. The Dialer Team

Supervisor reviews the Dialer daily to determine whether all scheduled collections calls are attempted. Prior to a loan going into foreclosure, the Pre-Foreclosure Manager completes the Pre-Foreclosure Checklist to determine whether the proper notification letters were sent to the borrower.

The term "Loss Mitigation" is intended to describe the full range of foreclosure prevention alternatives that may avert either the loss of a borrower's property to foreclosure, increased cost to the lender, or both. Loss Mitigation commonly consists of the following general types of agreements; Loan Modification, Deferment, Repayment Plan, Forbearance, Short Sale, or Deed in-Lieu. The terms of a loss mitigation solution will vary in each case according to the particular needs and goals of the parties. Clients are notified and provided additional information when they become 45 days or more delinquent.

The Loss Mitigation Department activities, including timelines, are conducted in accordance with applicable Federal, state, and local laws, agency and GSE guidelines, and Master Servicer-specific policies (e.g., CFPB, FNMA, FHLMC, FHA, VA, Master Servicer and private investor). The Loss Mitigation Department's goal is to determine whether there is a viable loan foreclosure prevention alternative for a borrower in default to resolve a mortgage delinquency and, if so, to assist the borrower in completing the loss mitigation process. Loss mitigation attempts are made before any loan is placed into foreclosure. A Loss Mitigation Checklist is used by the Loss Mitigation Department to ensure loss mitigation is handled according to agency and client guidelines.

DMI utilizes an on-line Foreclosure and Bankruptcy Tracking system. The system provides for detailed schedule of the processing of foreclosures and bankruptcies in each state. DMI utilizes this system to help monitor the performance of its attorneys. Clients utilizing the Remote Inquiry System can follow the foreclosing proceedings.

DMI reports on foreclosed loans to all major credit reporting agencies.

Standard Reporting

Master loan files are generated from MSP automatically as scheduled in a text file format. Standard reports are automatically generated based on predefined templates. Accuracy of data is ensured through proper report setup and configuration of the predefined templates. The following standard reports are most commonly used by user entities for financial reporting purposes:

- Customer Information File (CIF)
- General Ledger Report
- Report of Mortgage Loan Collections (P102)
- Monthly Statement of Mortgage Accounts (P139)
- Consolidation of Remittance Reports (S215)
- Trial Balance (P181)
- Loans Paid in Full (P110)
- Remittance Report (S210)

MSP allows scheduling up to 12 months. Scheduling of the MSP outputs is performed by IT annually to ensure completeness of outputs. Scheduling performed by IT applies to all clients in the system. A scheduler is in place to automatically import the MSP outputs to the data warehouse when a new output is detected. The Data warehouse automatically generates routine reports when new imports are detected. A scheduler is in place to automatically generate standard reports from the data warehouse. Reports are automatically generated by a standard template and rset table which uses client ID and investor code to identify the data with the respective client.

Standard reports generated are uploaded in client's FTP folders through an automatic scheduler. The automatic process of report generation ensures the accuracy and completeness of the report content. The report documents are archived on the client FTP sites for one year in a read only format.

Access to the automatic scheduler, client table, and data warehouse is restricted to authorized users.

Modifications to routine reports go through the standard change management procedure. DMI has implemented a software development life cycle (SDLC) policy which prescribes the authorization, development, UAT, and the final push to production. The SDLC policy is reviewed on an annual basis. All changes must be authorized by the Development team prior to development. All changes must be tested by an analyst. User Acceptance Testing (UAT) is completed as needed. All changes must be approved by a manager or team lead after testing, prior to migration into production.

F. Complementary User Entity Controls

Management of DMI assumed, in the design of DMI's subservicing operations system that certain controls will be implemented by user entities, and those controls are necessary, in combination with controls at DMI, to provide reasonable assurance that DMI's control objectives would be achieved. These complementary user entity controls and the related control objectives are described below. User entities are responsible for implementing such controls.

- User entities are responsible for maintaining proper controls over user IDs and passwords provided by DMI. (Objective 4)
- For electronic loan transfers and conversions, user entities and DMI will mutually agree upon the timing and extent of the due diligence procedures. User entities are responsible for reviewing all test data during the transfer process. (Objective 7)
- For all electronic new loan setups, user entities are responsible for reviewing the output reports daily, verifying that all loan information was included in the transfer, that the data transmitted properly, and that the data is accurate. (Objective 7)
- DMI requests copies of certain loan documents for loans other than conventional fixed rate loans. User entities are responsible for promptly providing these documents in order for DMI to compare key data elements to the loan setup transmission for accuracy. (Objective 7)
- After the initial development of an automated file-to-file application for flow loan transfers, user entities are responsible for providing copies of new loan information after the go-live date for up to 60 days to allow for an effective quality control audit. (Objective 7)
- User entities are responsible for paying all insurance and taxes due within 30 days of loan transfer. (Objective 7)
- User entities are responsible for notifying the investor of servicing transfer activities. (Objective 7)
- User entities that have elected not to have DMI perform an audit of special (ARM) loan setups following loan transfers are responsible for verifying accuracy of the loan's adjustable parameters. (Objective 8)
- User entities who send checks to DMI are responsible for including a Cash Transmittal Form. (Objective 8)
- User entities are responsible for verifying that all properties in special flood hazard areas have the correct insurance coverage amount at the time of transfer. (Objective 9)
- For loans that have undergone life of loan analysis, user entities are responsible for any interest rate rebates due to the borrower or investor. (Objective 9)
- User entities using DMI's general ledger interface are responsible for reconciling their general ledger accounts. (Objective 10)
- User entities who make withdrawals from or deposits into custodial accounts without specific instructions from DMI are responsible for reconciling that account. (Objective 10)
- User entities are responsible for promptly providing original documents or copies of documents (depending on state requirements) to initiate foreclosure. Additionally user entities need to provide any additional documentation requested by the court. (Objective 11)
- User entities are responsible for approving foreclosure recommendations for non-agency loans. (Objective 11)

- User entities are responsible for providing bidding instruction for the foreclosure sale for non-agency uninsured conventional loans. (Objective 11)
- User entities are responsible for promptly wiring HUD claim proceeds along with additional funds necessary to remit to the pool investor to liquidate the loan. (Objective 11)
- User entities are responsible for approving or denying loss mitigation workout recommendations for non-agency loans. (Objective 11)
- User entities are responsible for reviewing loss mitigation applications on a timely basis. (Objective 11)
- DMI does not provide legal advice. User entities are responsible for determining whether their institutional compliance and regulatory reporting requirements are satisfied. (Objective 12)
- User entities may need to assist with responses to inquiries or complaint that relate to prior servicing. (Objective 12)
- Recovery of DMI computing resources does not include client participation. User entities that interact directly with borrowers for activities such as payment collection and loan inquiry are responsible for developing internal procedures that identify their internal and external disaster recovery responsibilities in support of such activities. (Objective 13)

G. Control Objectives and Related Controls

The organization's control objectives and the related controls designed to provide reasonable assurance that the service organization's control objectives were achieved, are included in Section 4 of this report to eliminate the redundancy that would result from listing them in this section and repeating them in Section 4. Although the control objectives and related controls are presented in Section 4, they are an integral part of the entity level management process and description of system used to provide services.

Section 4. Dovenmuehle Mortgage, Inc.'s Description of its Control Objectives and Related Controls and Independent Service Auditor's Description of Tests of Controls and Results

This section presents the following information provided by Dovenmuehle Mortgage, Inc.:

- The control objectives specified by the management of DMI.
- The controls established and specified by DMI to achieve the specified control objectives.

Also included in this section is the following information provided by the service auditor:

- A description of the tests performed by the service auditor to determine whether the service organization's controls were operating with sufficient effectiveness to provide reasonable assurance that specified control objectives were achieved. The service auditor determined the nature, timing, and extent of the testing performed.
- The results of the service auditor's tests of controls.

The service auditor performed observation and inspection procedures as they relate to system-generated reports, queries and listings to assess the accuracy and completeness of the information used in the service auditor's tests of controls.

Testing performed and results of tests when using the work of internal audit

The Service auditors has used the work of the internal audit function (Internal Audit and Quality Assurance) of DMI to assist in determining the suitability of the design and operating effectiveness of the controls to achieve certain control objectives stated in the description to provide reasonable assurance that those control objectives were achieved throughout the period October 1, 2019 to September 30, 2020. Internal Audit and Quality Assurance were used to provide evidence for the following control objectives:

- Billing, Cashiering and Special Loan Servicing
- Escrow Processing
- Custodial Account Management
- Collections, Loss Mitigation and Foreclosure

The tests performed by Internal Audit and Quality Assurance are described in Section 3 of the report. No deviations were noted by Internal Audit and Quality Assurance. In addition to our assessment of the qualifications of the internal auditors and our review of their work for proper completion, service auditors reperformed selected tests that have been performed by members of the Internal Audit and Quality Assurance functions through a combination of independent testing and reperformance, and noted no deviations.

1. Organization and Administration

Control Objective: Controls provide reasonable assurance that the structure of the organization provides for management oversight and separation of duties and established policies and procedures with regards to information technology and performance of key business processes are communicated and adhered to.

Description of Controls

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
1. A formal management structure exists that defines levels of reporting and accountability. Assignment of responsibilities is made in order to segregate incompatible functions. The organization chart is made available to employees through the company's intranet.	**A.** Inspected the DMI organization chart to determine whether management and oversight functions are segregated.	**A.** No deviations noted.
	B. Inspected the company's intranet to determine whether the organization chart is made available to employees through the company's intranet.	**B.** No deviations noted.
2. The DMI Information Technology Department is divided into teams based on responsibilities and duties.	**A.** Inspected the DMI Technology Department organization chart to determine whether segregation of duties exist in information technology responsibilities and duties.	**A.** No deviations noted.
3. Monthly meetings are scheduled with senior vice presidents and department heads to review department operations, performance, and any outstanding issues.	**A.** Inspected meeting schedules for a sample of months to determine whether monthly meetings are scheduled with senior vice president and department heads to review department operations, performance, and any outstanding issues..	**A.** No deviations noted.
4. An employee handbook exists to serve as a guide for DMI employees. The manual provides a basic	**A.** Inspected the DMI Employee Handbook to determine whether it communicates the company's philosophy, procedures, and operating policies.	**A.** No deviations noted.

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
understanding of the company's philosophy, procedures, and operating policies. DMI employees are required to sign an acknowledgement during time of hire to indicate that they have read and will comply with the policies as stated in the handbook.	**B.** Inspected employee handbook acknowledgement forms for a sample of new hires to determine whether employees are required to read and acknowledge the handbook.	**B.** No deviations noted.
5. An Information Security Policy (ISP) exists that documents employee responsibilities for the use of DMI technology, programs, files, unauthorized use of passwords, and the appropriate use of the Internet. Security Awareness Training is provided to employees upon hire and on an annual basis to ensure the ISP is effectively communicated to employees.	**A.** Inspected the ISP to determine whether it defines the use of DMI technology, programs, files, unauthorized use of passwords, and the appropriate use of the Internet.	**A.** No deviations noted.
	B. Inspected Security Awareness Training completion forms for a sample of employees to determine whether Security Awareness Training is provided to employees on an annual basis.	**B.** **Deviations noted.** Annual security awareness training was not completed during the reporting period for 4 of 20 employees selected for testing.
	C. Inspected Security Awareness Training completion forms for a sample of new hires to determine whether Security Awareness Training is provided to employees upon hire.	**C.** No deviations noted.
6. All DMI employees are required to sign a confidentiality agreement at the time of hire stating that they will keep all client information, all mortgagor information, and any other private information strictly confidential.	**A.** Inspected confidentiality agreements for a sample of new hires to determine whether employees are required to acknowledge and sign confidentiality agreements at the time of hire.	**A.** No deviations noted.

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
7. Background checks are performed by HR on every DMI employee upon hiring. Background checks cover federal and state violations and financial history.	**A.** Inspected background check reports for a sample of new hires to determine whether background checks are performed for all employees upon hire.	**A.** No deviations noted.
8. The DMI Training Department provides annual training to all employees on protecting customer information with a focus on the requirements of and compliance with the Gramm-Leach-Bliley Act.	**A.** Inspected GLBA training completion forms for a sample of employees to determine whether GLBA training is provided on an annual basis.	**A.** **Deviations noted.** Annual GLBA training was not completed during the reporting period for 5 of 20 employees selected for testing.
9. DMI has a Subservicing Policy Manual that describes the basics of each of the services that DMI will provide for clients and describes the client's responsibilities relating to that service. The Subservicing Policy Manual is provided to clients at the time of onboarding. Updates to the manual are provided to clients through DMIConnect.	**A.** Inspected the Subservicing Policy Manual to determine whether each of the DMI services is described and client responsibilities are outlined where applicable.	**A.** No deviations noted.
	B. Inspected the Subservicing Policy Manual acknowledgment forms for a sample of new clients to determine whether it is communicated to clients at the time of onboarding.	**B.** No deviations noted.
	C. Observed the DMIConnect site to determine whether updated versions of the manual are provided to clients through DMIConnect.	**C.** No deviations noted.
10. Each DMI department that performs mortgage subservicing activities has written standards and procedures documents, and reviews them on an annual	**A.** Inspected standards and procedures documents for a sample of departments to determine whether the documents that describe departmental procedures exist.	**A.** No deviations noted.

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
basis. The documents are made available to employees through the company's internal document management portal. Those departments include: • Bank reconciliations • Cashiering • Claims, REO, Property Preservation • Collections • Corporate Training • Customer service • Default Reporting • Escrow Administration • Human Resources • Internal Revenue Code Reporting • Investor accounting • Loss mitigation • Mortgage disposition • Records/Mailroom • Research & Release • Special Loans • Transfers & Conversions	**B.** Inspected the internal document management portal to determine whether standards and procedures documents are made available to all employees.	**B.** No deviations noted.
	C. Inspected the review of the standards and procedures documents for a sample of DMI departments to determine whether they are reviewed on an annual basis.	**C.** No deviations noted.

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
11. DMI has a Quality Assurance Department that based on the department’s risk, conducts a monthly, quarterly and/or annual reviews in the following areas: • Bank reconciliations • Cashiering • Claims, REO, Property Preservation • Collections • Corporate Training • Customer Service • Default reporting • Escrow Administration • Human Resources • Internal Revenue Code Reporting • Investor accounting • Loss mitigation • Mortgage disposition • Records/Mailroom • Research & Release • Special Loan Transfers & Conversions	**A.** Inspected quality assurance reports for a sample of departments to determine whether reviews are performed on a monthly, quarterly, or annual basis.	**A.** No deviations noted.

2. Physical Security

Control Objective: Controls provide reasonable assurance that physical access to the computer equipment, storage media, program documentation, and hard copy of computer data containing customer information is limited to authorized personnel.

Description of Controls

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
1. Dovenmuehle has offices in three locations: Lake Zurich, IL, North Aurora, IL, and Elgin, IL. Access to all facilities is controlled by an electronic key card system.	**A.** Observed operation of the Lake Zurich, North Aurora, and Elgin buildings to determine whether access to the DMI office suites is controlled by electronic key cards.	**A.** No deviations noted.
2. All visitors to the Lake Zurich facility must sign in at the security desk and present their identification. Visitors must be escorted by a DMI employee. Similarly, visitors to the Elgin facility must sign the visitors' log and be escorted by a DMI employee. Visitors to the North Aurora facility must be escorted by a DMI employee at all times. Visitor badges are provided to Lake Zurich visitors. All electronic key cards for visitors are accounted for each day by the building security. Any missing cards are deactivated each night.	**A.** Observed the visitor sign-in process at the Lake Zurich building to determine whether visitors are required to provide a valid photo ID, wait to be escorted by a company representative, or be authorized to be sent up to the office receptionist.	**A.** No deviations noted.
	B. Observed the visitor sign-in process at the Elgin and North Aurora facilities to determine whether visitors are required to be escorted by a company representative.	**B.** No deviations noted.
	C. Performed corroborative inquiry with the building security of the Lake Zurich facility and the Senior Vice President of Risk Management to confirm our understanding that any visitor electronic access cards that are unaccounted for are deactivated at the end of each business day.	**C.** No deviations noted.

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
3. Access cards for the Lake Zurich building are maintained by building security. DMI administers the badge system in Elgin and North Aurora. Administrative access to the badge systems at Elgin and North Aurora are limited to HR, Executive Support/Business Continuity and the Facilities Manager. Access cards and access levels are granted based upon an Access Card Request form that is submitted by DMI. The HR department conducts a quarterly review of access levels to the building and suite for all three office locations.	**A.** Inspected the Access Card Request form for a sample of new hires to determine whether badge access is authorized.	**A.** No deviations noted.
	B. Inspected a system generated list of users with administrative access to the badge system in Elgin and North Aurora to determine whether access is restricted as stated in the control description.	**B.** No deviations noted.
	C. Inspected the access review performed by Human Resources for all three facilities for a sample of quarters to determine whether badge access is reviewed on a quarterly basis.	**C.** No deviations noted.
4. The Lake Zurich building has a burglar alarm that is monitored 24/7 by the building's security agency. The Elgin and North Aurora offices have burglar alarms that are monitored 24/7 by TYCO. The Lake Zurich, North Aurora, and Elgin office buildings have video cameras monitoring all entry points.	**A.** Performed corroborative inquiry with building security for the Lake Zurich, North Aurora and Elgin facilities and the Senior Vice President and IT Security Compliance Analyst to confirm our understanding that the alarm systems are monitored 24/7.	**A.** No deviations noted.
	B. Observed operation of the Lake Zurich, North Aurora, and Elgin building video camera systems to determine whether camera systems exist to monitor entry points.	**B.** No deviations noted.

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
5. The Lake Zurich and North Aurora data centers house all production computer equipment and the phone system. The data centers are located in secure areas of DMI facilities, away from exterior exits. Access to the data centers is controlled via proximity badge and key pad combination code that is unique to each individual with access. Access is restricted to members of the Information Technology Department and Executive Management.	**A.** Observed the access controls for the data centers at Lake Zurich and North Aurora to determine whether the data secure is located in secure areas of DMI facilities, away from exterior exits, access is controlled via proximity badge and electronic key code, and that the door to the data center is kept locked.	**A.** No deviations noted.
	B. Inspected a system generated list of individuals with access to the Lake Zurich and North Aurora data centers and inspected individuals' job titles to determine whether access is restricted to authorized members of Executive Management and Information Technology.	**B.** No deviations noted.
6. The DMI Cashiering Department is located in a secure location within the Lake Zurich suite. Access to the Cashiering Department is controlled by an electronic badge system. Access to the Department is limited to Cashiering Department employees. Select IT Staff also require access for technical support purposes.	**A.** Observed the access control to the Cashiering Department to determine whether access is controlled via an electronic badge.	**A.** No deviations noted.
	B. Inspected a system generated list of individuals with access to the Cashiering Department and the related job titles for a sample of individuals to determine whether access is restricted based on individuals' job responsibilities.	**B.** No deviations noted.

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
7. DMI utilizes an employee Term Notice/Checklist form to manage the process of terminating an employee. The form includes collecting the electronic swipe cards for all locations. The Human Resource Department notifies Lake Zurich building security of all terminations at the Lake Zurich location and the Manager in Elgin and North Aurora of all terminations at the Elgin and North Aurora locations and access is revoked within one business day.	**A.** Inspected termination checklists for a sample of terminated employees to determine whether access is revoked upon termination within one business day.	**A.** No deviations noted.

3. Environmental Security

Control Objective: Controls provide reasonable assurance that computer equipment and storage media are protected from environmental factors.

Description of Controls

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
1. The Lake Zurich, North Aurora, and Elgin facilities are monitored 24/7 by a fire detection system. The systems are monitored by the respective local fire departments.	**A.** Observed the fire alarm system controls at all facilities and performed a corroborative inquiry with management to determine whether fire alarm system controls exist at all facilities and facilities are monitored by the local municipal fire departments.	**A.** No deviations noted.
2. Fire extinguishers are placed throughout the Lake Zurich, North Aurora, and Elgin office facilities according to local fire code. The Lake Zurich and North Aurora data centers are equipped with smoke detectors and electrically rated fire extinguishers. All fire extinguishers are serviced at least annually.	**A.** Observed all facilities to determine whether fire extinguishers are present throughout the office facilities.	**A.** No deviations noted.
	B. Observed the data centers at the Lake Zurich and North Aurora facilities to determine whether electrically rated fire extinguishers and smoke detectors are installed in the data centers.	**B.** No deviations noted.
	C. Inspected documentation of the most recent fire extinguisher inspection for all facilities to determine whether fire extinguishers are serviced at least annually and during the reporting period.	**C.** No deviations noted.
3. The data centers in Lake Zurich and North Aurora are temperature controlled via dedicated HVAC systems. Temperature sensors are in place and configured to send alerts to IT personnel when	**A.** Observed the data centers at Lake Zurich and North Aurora facilities to determine whether dedicated HVAC systems are installed.	**A.** No deviations noted.
	B. Inspected the temperature alert settings for Lake Zurich and North Aurora data centers to determine whether temperature is monitored.	**B.** No deviations noted.

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
the temperature rises above a certain threshold. Servers are protected from power surges, brownouts, and failures through the use of an uninterruptible power supply (UPS) unit. The UPS maintains server power and provides for a controlled shutdown of the servers. UPS units are scheduled to perform self-tests every two weeks.	**C.** Observed the data centers at Lake Zurich and North Aurora facilities to determine whether production systems are connected to the UPS units.	**C.** No deviations noted.
	D. Inspected the UPS settings for Lake Zurich and North Aurora data center to determine whether UPS units are scheduled to perform self-tests every two weeks.	**D.** No deviations noted.
4. The data center located in Lake Zurich is located on the third floor of the building to protect against flooding. The data center has a raised floor and equipment is stored on equipment racks. Equipment is stored on equipment racks at the backup data center in North Aurora.	**A.** Observed the Lake Zurich data center to determine whether it is located on the third floor to protect against flooding.	**A.** No deviations noted.
	B. Observed the Lake Zurich and North Aurora data centers to determine whether equipment is stored on equipment racks.	**B.** No deviations noted.

4. Logical Access

Control Objective: Controls provide reasonable assurance that logical access to applications and data is limited to authorized individuals.

Description of Controls

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
1. Logical access is divided into two areas, the Local Area Network (LAN) and the MSP application. Logical access is controlled via unique user IDs and passwords. The LAN password policy requires passwords to be a minimum of eight characters, to expire every 45 days, and to meet complexity requirements. The last 24 passwords cannot be reused. After five incorrect password attempts, the account is locked out for 15 minutes. A screen saver is enabled after 10 minutes of inactivity. The MSP password policy requires a minimum of eight alphanumeric characters, must meet complexity requirements and expire at least every 90 days. The account sessions time out after 20 minutes of inactivity.	**A.** Inspected the LAN authentication parameters to determine whether LAN password parameters are configured as stated in the control description.	**A.** No deviations noted.
	B. Inspected the MSP authentication standards to determine whether MSP password parameters are configured as stated in the control description.	**B.** No deviations noted.
2. New hire access requests are performed using a completed security request form.	**A.** Inspected access request forms for a sample of new hires to determine whether access is authorized by a manager.	**A.** No deviations noted.

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
Department managers must complete and approve the form. Requests are processed by the Technology Department.	**B.** Inspected access request help desk tickets for a sample of new hires to determine whether access is provisioned by the Technology Department as requested.	**B.** No deviations noted.
3. Employees are only granted VPN access if approved by their department manager in a security request form. Secured token and 2048 bit connection is required for VPN access. A 15 minute inactivity timeout is in place.	**A.** Inspected access request forms for a sample of users granted VPN access during the period to determine whether access is authorized by the department manager.	**A.** No deviations noted.
	B. Observed a user login to the VPN to determine whether a token is required.	**B.** No deviations noted.
	C. Inspected the VPN site certificate to determine whether 2048-bit encryption is required for remote access.	**C.** No deviations noted.
	D. Inspected the VPN configuration to determine whether a 15 minute inactivity timeout is enforced.	**D.** No deviations noted.
4. The Systems Department is notified of employee terminations at the time of termination through the help desk system and access is revoked by Helpdesk within two business days. After three days of unexplained absence, employees are terminated. For employees resigning without notice, the LAN and MSP user accounts are deleted within five business days of their last day worked.	**A.** Inspected termination requests for a sample of terminated employees to determine whether the Systems Department is notified of terminations.	**A.** No deviations noted.
	B. Inspected Help Desk tickets for a sample of terminated employees to determine whether the employees' user IDs are removed or deactivated for both the LAN and MSP within two business days, or within five business days for employees with unexplained absences.	**B.** No deviations noted. ●

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
5. DMI network administrative access is limited to members of the Systems Department that require that level of access to perform their job duties. Administrator level access to the MSP system is limited to only those authorized individuals requiring that level of access to perform their job duties.	**A.** Inspected a system generated list of users with DMI network administrative access rights to determine whether access is restricted to authorized users based on job functions.	**A.** No deviations noted.
	B. Inspected a system generated list of users with MSP administrative access to determine whether access is restricted to authorized users based on job functions.	**B.** No deviations noted.
6. IT sends Active Directory and MSP user lists to department managers for review on a quarterly basis. Department managers review the listings to ensure access levels are appropriate and only authorized users have access.	**A.** Inspected Active Directory and MSP user access reviews for a sample of departments and quarters to determine whether access reviews are performed by department managers quarterly.	**A.** No deviations noted.
7. Firewalls are in place to control and limit the type of network traffic allowed in and out of the network.	**A.** Inspected the DMI network diagram to determine whether firewalls exist between DMI's internal network and the Internet.	**A.** No deviations noted.
	B. Inspected firewall rule sets to determine whether the firewalls are configured to control and limit the type of network traffic allowed in and out of the network.	**B.** No deviations noted.

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
8. Clients access their reports and upload new files via a Client Portal web connection. Three emails are sent out to the client by IT Helpdesk when new accounts are created. One includes the RIS Client Manual, the second consists of the username, and the third indicates the end-user's password.	**A.** Inspected templates of the emails sent to clients to determine whether the clients' initial contact, username, and password are sent separately.	**A.** No deviations noted.
9. Clients are granted remote access through a web interface based on an authenticated ID upon authorization from the client. User accounts for client access to the MSP system are restricted from accessing loan information of other clients. The web interface is secured with TLS encryption. In addition, client's IP address ranges are hardcoded in the firewall rule set to explicitly allow traffic only from preauthorized sources.	**A.** Inspected user access requests for a sample of new clients to determine whether user accounts are authorized by the client.	**A.** No deviations noted.
	B. Inspected system configurations to determine whether clients are restricted from accessing information of other clients in MSP.	**B.** No deviations noted.
	C. Observed a user access the web interface to determine whether TLS encryption is used.	**C.** No deviations noted.
	D. Inspected firewall rule sets for a sample of clients to determine whether client IP address ranges are hardcoded to explicitly allow traffic only from preauthorized sources.	**D.** No deviations noted.

5. System Maintenance, Monitoring and Change Management

Control Objective: Controls provide reasonable assurance that systems are monitored for performance, maintenance, capacity and security issues; that system software is kept at current release and patch levels; and that change requests to MSP are authorized, tested, and approved.

Description of Controls

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
1. Authorization to request changes to MSP is limited to the MSP group. MSP sends Update Advisories to DMI when new versions of the software are available. IT Helpdesk tests updates as necessary from MSP before installing necessary updates.	**A.** Inspected a system generated list of users authorized to request changes to MSP to determine whether access is restricted to the MSP group.	**A.** No deviations noted.
	B. Inspected the Update Advisories sent to DMI and evidence of testing and implementation for a sample of Update Advisories to determine whether updates are sent to DMI and tested by IT Helpdesk for implementation as necessary.	**B.** No deviations noted.
2. All DMI file servers, routers, and network devices are monitored by the IT Network Security Team for system events. The PRTG Network Monitoring software is configured to alert the Systems Department via cell phone of the occurrence of certain events or performance thresholds. Resolution and uptime status are tracked within the PRTG Monitoring software dashboard. The network monitoring software also monitors uptime, bandwidth, and system capacity.	**A.** Inspected the PRTG Network Monitoring software configurations and monitoring dashboard to determine whether the system is configured to send notifications via cell phone in the event of an alert to the Systems Department and track the resolution and uptime status of certain events and performance thresholds.	**A.** No deviations noted.
	B. Inspected the PRTG Network Monitoring software to determine whether the software monitors uptime, bandwidth, and system capacity monitoring.	**B.** No deviations noted.

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
3. DMI servers and workstations running the Microsoft operating system are updated via the Windows Software Update Services (WSUS).	**A.** Inspected the patch levels for a sample of servers and workstations to determine whether critical updates are installed.	**A.** No deviations noted.
4. Antivirus software is installed on all DMI servers and workstations. The software scans machines for viruses in real-time.	**A.** Inspected antivirus software virus definition files for a sample of DMI servers and workstations to determine whether antivirus software is installed and configured to automatically update.	**A.** No deviations noted.
5. Access to make changes to the firewall is restricted to network administrators.	**A.** Inspected a system generated list of firewall administrators to determine whether access is restricted to network administrators.	**A.** No deviations noted.
6. Firewall logs are retained for at least 60 days to provide for forensic investigation.	**A.** Inspected the firewall log to determine whether logs are retained for at least 60 days.	**A.** No deviations noted.
7. An Intrusion Detection System (IDS) and/or Intrusion Protection System (IPS) is in place to detect suspicious activity. It is configured to notify the IT Department of suspicious activities. Alerts are investigated by the IT Department and resolution is tracked within the ticketing system.	**A.** Inspected the IDS/IPS console to determine whether the system is configured to send alerts to the IT Department when suspicious activity is detected.	**A.** No deviations noted.
	B. Inspected help desk tickets for a sample of IDS/IPS alerts to determine whether they are investigated and tracked to resolution.	**B.** No deviations noted.
8. DMI has implemented a software development life cycle (SDLC) policy which prescribes the authorization, development, UAT, and the final push to production. The SDLC policy is reviewed by the IT team on an annual basis.	**A.** Inspected the SDLC policy to determine whether it is formally documented and was reviewed by the IT team annually.	**A.** No deviations noted.

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
9. All changes must be authorized by a Team Lead or Manager prior to development.	**A.** Inspected the change tickets for a sample of changes to determine whether changes are authorized by a Team lead or Manager prior to development.	**A.** No deviations noted.
10. All changes must be tested by development staff, project management, or client based on the request type.	**A.** Inspected the change tickets for a sample of changes to determine whether testing is performed.	**A.** No deviations noted.
11. All changes must be approved by the Development Manager or Director of IT after testing, prior to migration into production.	**A.** Inspected the change tickets for a sample of changes to determine whether all changes are approved by the Development Manager or Director of IT prior to being moved into production.	**A.** No deviations noted.

6. Vendor Management

Control Objective: Controls provide reasonable assurance that critical vendors are identified and performance is evaluated in accordance with the vendor management policy.

Description of Controls

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
1. DMI has a vendor management program that identifies critical vendors and their functions and cross-references the vendors to the appropriate DMI department. The CFO assesses vendors for criticality classification on an annual basis and documents the assessment in the Critical Vendor Listing with Rotational Review Breakout.	**A.** Inspected the DMI Vendor Management Policy to determine whether a vendor management policy exists.	**A.** No deviations noted.
	B. Inspected the Critical Vendor Listing with Rotational Review Breakout to determine whether the assessment identifies key vendors and the services provided.	**B.** No deviations noted.
	C. Inspected the Critical Vendor Listing with Rotational Review Breakout to determine whether vendor criticality is assessed and the rotational review schedule is determined by the CFO on an annual basis.	**C.** No deviations noted.
2. DMI enters into a service contract with all key third-party vendors. DMI has identified all vendors with access to confidential customer information. Upon initiation, the Legal Department and the related Operational Management completes the Vendor Contract Review Checklist to ensure each vendor contract includes a confidentiality agreement, business resumption and contingency plans, the right to audit performance and GLBA compliance.	**A.** Inspected Vendor Contract Review Checklists performed by the Legal Department and the related Operational Management for a sample of critical vendors to determine whether each vendor contract includes a confidentiality agreement, business resumption and contingency plans, the right to audit performance and GLBA compliance.	**A.** No deviations noted.

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
3. DMI performs vendor assessments for all critical vendors on an annual basis. The Internal Audit reviews vendor SOC or ITGC reports to verify there are no significant deviations related to services being provided to DMI and the CFO reviews the financial statements of the vendor to determine whether the vendor is solvent and evaluates vendor overall performance against the objectives specified in service level agreements.	**A.** Inspected vendor assessment documentation packages for a sample of critical vendors to determine whether a performance review, including a review of the vendor's SOC or ITGC reporting and financial statements is performed by the Internal Audit Team and the CFO on an annual basis.	**A.** No deviations noted.

7. Loan Setup

Control Objective: Controls provide reasonable assurance that data is loaded into the system accurately and completely and that all loan parameters and beginning balances agree to the information provided by the client.

Description of Controls

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
1. DMI users automated file-to-file transfers for loading loans (also known as boarding). The file-to-file loan transfer procedures are documented in New Loan Setup Guide documents.	**A.** Inspected the New Loan Setup Guides for interface boarding to determine whether loan setup procedures exist and are documented.	**A.** No deviations noted.
2. When new file-to-file loans are received by DMI, an automatic email is sent to the Electronic Loan Interface (ELI) Proxy mailbox. The Coordinators check the inbox several times per day and move the e-mails from the inbox to the client's appropriate folder as the loans are boarded.	**A.** Performed corroborative inquiry with the Assistant Manager and the Internal Audit Supervisor to confirm our understanding that the mailbox is checked several times per day to ensure new loans are received and boarded.	**A.** No deviations noted.
	B. Observed a Coordinator access the ELI inbox to determine whether emails sent to the ELI Proxy mailbox are filed into the appropriate client folders.	**B.** No deviations noted.

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
3. All electronic loan files are loaded into the DMI New Loan Interface (NLI) or MSP ELI. Data loaded into NLI is received from clients and requires data mapping prior to loading. Data loaded into ELI is received from the client in pre-mapped spreadsheets. For NLI, the following controls are in place to determine whether the data mapping is performed accurately and completely: 1) Data is loaded into a test environment by Data Mappers and reviewed by New Loan Setup Auditors for data mapping, file integrity, cash balances, interest rate parameters and total loan count. 2) The customer must approve the data mapping prior to loading into the live environment. For ELI, the customer is responsible for reviewing the accuracy and completeness of data loaded into the live environment.	**A.** Inspected NLI tracking sheets for a sample of NLI implementations to determine whether test loads are performed and reviewed by New Loan Setup Auditors.	**A.** No deviations noted.
	B. Inspected customer approval for a sample of NLI implementations to determine whether customer approval is obtained prior to go-live.	**B.** No deviations noted.

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
4. Once loans are loaded into the live environment, New Loan Setup Auditors review 100% of all loan fields for loans loaded during the first 90 days. Daily audits are documented in weekly audit spreadsheets. Tasks are created for all issues identified during the daily audits. New Loan Setup Supervisors are responsible for monitoring the Open Task Queue continuously throughout the day to determine whether issues are resolved.	**A.** Inspected weekly audit spreadsheets for a sample of NLI implementations to determine whether loan files are reviewed for accuracy for 90 days.	**A.** No deviations noted.
	B. Observed the tasks within the Open Task Queue dashboard and inquired with New Loan Setup Supervisors to confirm our understanding that supervisors monitor the resolution of open tasks continuously throughout the day.	**B.** No deviations noted.

8. Billing, Cashiering and Special Loan Servicing

Control Objective: Controls provide reasonable assurance that loan payments are received and processed accurately, completely, and securely and that special loan servicing is accurate and complete.

Description of Controls

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
1. The Print Vendor Liaison sends daily statements or weekly coupon book requests to a vendor for printing and mailing. Daily and weekly reconciliations are performed by the Print Vendor Liaison to ensure payment coupon books and billing statements are printed and mailed out timely.	**A.** Inspected billing statement report reconciliations for a sample of days to determine whether the reconciliations are performed by the Print Vendor Liaison daily.	**A.** No deviations noted.
	B. Inspected coupon book report reconciliations for a sample of weeks to determine whether the reconciliations are performed by the Print Vendor Liaison weekly.	**B.** No deviations noted.
2. Loan payments are received by check, ACH or online payment. **Checks:** Lockbox checks are opened in a secure room that is controlled via key pad code. Access is limited to Cashiering personnel. Checks are then transferred to the Cashiering Department for processing. At the end of each day, all checks are locked in the Cashiering Department in a fire proof safe which is restricted to authorized Cashiering Department personnel. Daily, DMI lockbox checks are imaged and processed using	**A.** Observed the mail area operation to determine whether access is controlled via key pad code.	**A.** No deviations noted.
	B. Inquired with the Cash Processing Supervisor to determine whether access to the mail area is restricted to Cashiering personnel.	**B.** No deviations noted.
	C. Observed checks being stored inside the fire proof safe and inquired with the Cash Processing Supervisor to determine whether checks are stored in the safe at the end of each day and access to the safe is restricted to authorized Cashiering Department personnel.	**C.** No deviations noted.
	D. Observed a Cashiering employee create a payment error to determine whether payments are sent to a rejection queue.	**D.** No deviations noted.

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
the MaxPay application. The loan number and amount are keyed by Cashiering employees during the imaging process. After imaging, payments are batched and posted to MSP. Payments that are rejected by the system are automatically sent to the appropriate rejection queue for review. At the end of each day, payments that can be posted to MSP are encoded and endorsed for deposit into the bank. Quality Control employees compare the check amount with the amount encoded to ensure payments are posted accurately. Payments that remain unresolved are populated on the Payments Pulled Report, investigated, and resolution is documented in the MSP loan history	**E.** Inquired with Cash Processors and observed the monitoring process to determine whether rejection queues are monitored continuously throughout the day for timely resolution of rejected payments.	**E.** No deviations noted.
	F. Observed the QC process operation to determine whether the check amount is compared to the amount encoded.	**F.** No deviations noted.
	G. Inspected the Payment Pulled Report for a sample of payments to determine whether resolutions are documented in the MSP Loan History.	**G.** No deviations noted.
3. ACH: ACH payments are batched and auto-posted to MSP. Payments that do not post automatically are sent to the suspense account. On a weekly basis, Aged Suspense Reports are sent to the departments affected for review. **Online Payment:** The online system used by borrowers to make payments is secured via HTTPS encryption.	**A.** Inspected email evidence for a sample of weeks to determine whether Aged Suspense Reports are sent to the departments affected for review.	**A.** No deviations noted.
	B. Inspected encryption settings for the online site managed by DMI to determine whether HTTPS encryption is used.	**B.** No deviations noted.

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
4. For each cash receipt, the cash processor reconciles the total amount of borrower cash receipts processed with the batch total posted to the system.	**A.** Inspected reconciliations for a sample of cash receipts to determine whether cash receipts are reconciled to batch totals posted to the system daily.	**A.** No deviations noted.
5. The Special Loans Department tracks interest rate indices. Rates are checked daily and the MSP system is updated when rate changes occur. The Special Loans Department verifies that the daily ARM rate adjustments are made in accordance with the proper index, look-back calculation method, remaining term, and rounding. A hard copy of the actual interest rate table that the rate change was based upon is scanned into DMI's system and retained indefinitely.	**A.** Inspected a sample of interest rate tables to determine whether the MSP system is updated when rate changes occur.	**A.** No deviations noted.
	B. Inspected the rate history for a sample of interest rate tables and evidence that a secondary individual verified the index value to determine whether ARM rate adjustments are verified.	**B.** No deviations noted.
	C. Inspected interest rate table history on-line to determine whether historical rate tables are retained.	**C.** No deviations noted.
6. Date of rate change and index lead days are maintained within MSP for ARM loans. A daily report is run to identify loans requiring rate changes. The Special Loans Supervisor reviews daily reports and verifies that rate changes were calculated accurately by the system.	**A.** Inspected rate change reports for a sample of days to determine whether the Special Loans Supervisor reviews daily reports and verifies that rate changes are calculated accurately by the system.	**A.** No deviations noted.
7. When ARM loans require first-time rate changes, indices are reviewed by the Special Loans Department against loan terms, calculated, and updated in MSP.	**A.** Inspected a sample of ARM loans requiring first-time rate changes to determine whether indices are updated and reviewed by the Special Loans Department for accuracy.	**A.** No deviations noted.

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
8. System tapes used to prepare notification letters are generated automatically every five business days. Each week the total number of loans adjusted is compared to the total number of letters sent. If the numbers do not agree, the loans that have not had a letter generated are investigated and a manual notification letter is prepared and sent. If a tape is not released for 5 business days, the system will automatically release the tape to the vendor for printing.	**A.** Inspected the ARM Vendor Tape Control Program for a sample of weeks to determine whether system tapes are prepared at least every five business days.	**A.** No deviations noted.
	B. Inspected weekly total reports for a sample of weeks to determine that the total number of loans adjusted is compared to the total number of letters sent.	**B.** No deviations noted.
	C. Inspected system configurations for ARM notices to determine whether the system will automatically release tapes to vendors if they are not sent by DMI within 5 business days.	**C.** No deviations noted.
9. Loan payoff processing by the Release Department includes a calculation and check of interest due and the generation of a payoff letter that lists principal, interest, and any escrowed amounts due.	**A.** Inspected payoff letters for a sample of paid-off loans to determine whether payoff letters are prepared by the Release Department and included principal, interest, and any escrow due.	**A.** No deviations noted.

9. Escrow Processing

Control Objective: Controls provide reasonable assurance that escrow accounts are processed accurately, that account balances are correct, that escrow disbursements are timely, and that interest payments and excess amounts are processed accurately. Controls also provide reasonable assurance that checks are secured and authorized.

Description of Controls

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
1. A trial analysis is run by the Escrow Department prior to the scheduled annual analysis, and exception reports are reviewed and corrected. The process is repeated until all errors are resolved.	**A.** Inspected the trial analysis and annual analysis for a sample of loans on the open items report to determine whether the loan analysis is performed and any errors are resolved after the final analysis.	**A.** No deviations noted.
2. All non-escrowed loans are reviewed by the Escrow Department annually to make sure tax payments are current. DMI communicates with the borrower on all loans with delinquent taxes. If the borrower does not bring the taxes current, DMI will pay the tax and establish an escrow for the loan.	**A.** Inspected the MSP history for a sample of tax delinquent loans to determine whether tax delinquency notifications are sent to the borrower.	**A.** No deviations noted.
	B. Inspected the MSP history for a sample of tax delinquent loans to determine whether DMI establishes an escrow account for the loan if the taxes are not brought current.	**B.** No deviations noted.
3. DMI's legal department conducts a quarterly review for all states requiring interest payments on escrow and interest payments are adjusted as necessary.	**A.** Inspected documentation of the review by the legal department for a sample of quarters to determine whether the legal department conducts a quarterly review for all states requiring interest payments on escrow to ensure interest payments are adjusted as necessary..	**A.** No deviations noted.

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
4. The Escrow Department performs an annual escrow analysis for each escrowed loan in order to determine that the current required escrow balance is never less than the minimum escrow balance.	**A.** Inspected the escrow analysis performed for a sample of escrow loans to determine whether an escrow analysis is performed annually at its anniversary period and within the report period.	**A.** No deviations noted.
5. The annual escrow analysis includes calculations to determine if there is excess escrow. At the conclusion of the escrow analysis process, if there are no errors or stops and excess escrow has been calculated, the system will automatically generate a refund check to the borrower for any excess escrow above $50. The Escrow Analysis Representative's review of daily Delinquent Loans with Overage reports is reported upwards to the Escrow Manager on a monthly basis, using the Analysis Work Schedule.	**A.** Inspected MSP escrow analysis options configurations to determine whether checks are automatically generated for excess escrow above $50.	**A.** No deviations noted.
	B. Inspected the Analysis Work Schedule for a sample of months to determine whether the Escrow Analysis Representative reports the review of the Delinquent Loans with Overage reports to the Escrow Manager on a monthly basis.	**B.** No deviations noted.
6. Loans paid in full are automatically analyzed for remaining escrow balances. Positive balances in escrow are automatically refunded to borrowers.	**A.** Inspected the Mortgage Loan History report for a sample of loans to determine whether paid-in-full loans with positive escrow are analyzed.	**A.** No deviations noted.
	B. Inspected check payment for a sample of loans to determine whether unpaid escrow balances are refunded.	**B.** No deviations noted.
7. The check printer and check stock are stored in a secure	**A.** Observed the check printer and check stock to determine whether both are secured in the data closet.	**A.** No deviations noted.

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
room that is secured via physical key lock. Authorized DMI check signers are limited to the CFO and Senior Vice Presidents.	**B.** Inspected list of authorized check signors to determine whether access is limited to authorized individuals.	**B.** No deviations noted.

10. Custodial Account Management

Control Objective: Controls provide reasonable assurance that account reconciliations are monitored for completeness and accuracy.

Description of Controls

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
1. The Bank Reconciliation Department utilizes DMI's Bank Account Manager application to track the status of all custodial bank accounts requiring reconciliation. The AVP of Bank Reconciliations monitors account reconciliations for completeness throughout the month.	**A.** Observed the Bank Account Manager application in operation and inquired with the Assistant Manager of Bank Reconciliations to determine whether the Bank Reconciliation Department utilizes DMI's Bank Account Manager application to track the status of all custodial bank accounts requiring reconciliation and the AVP of Bank Reconciliations monitors account reconciliations for completeness throughout the month.	**A.** No deviations noted.
2. All custodial accounts are reconciled monthly by authorized personnel. Reconciliations are approved by the department manager, assistant manager, or supervisor.	**A.** Inspected bank reconciliations for a sample of accounts and months to determine whether bank reconciliations are performed monthly and approved by either the department supervisor or manager.	**A.** No deviations noted.

11. Collections, Loss Mitigation and Foreclosure

Control Objective: Controls provide reasonable assurance that processing of delinquent accounts is in accordance with applicable servicing guidelines; that delinquent accounts undergo loss mitigation procedures prior to being referred for foreclosure; and that applicable federal, state, and client guidelines are followed for accounts placed in foreclosure.

Description of Controls

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
1. Clients are notified by mail and provided additional information when they become 45 days or more delinquent. The Loss Mitigation Department monitors the letters that are prepared to be sent out daily for quality, completeness, accuracy, and timeliness.	**A.** Inspected system design documentation to determine whether letters are automatically generated when accounts become delinquent.	**A.** No deviations noted.
	B. Inspected the Loss Mitigation quality control log for a sample of days to determine whether letters are monitored for quality, completeness, accuracy, and timeliness.	**B.** No deviations noted.
2. The Collections Department monitors and follows the collection guidelines set forth by FNMA. Specific FHLMC, FHA, VA, and client guidelines are followed as required. DMI has published Collection Timetables in the Subservicing Policy Manual.	**A.** Inspected the Subservicing Policy Manual to determine whether the Collection Timetable details the time frames and specific collection techniques to be performed based upon the type of loan.	**A.** No deviations noted.
3. Collection processing follows the guidelines established in the Collections Policy and Procedures to notify borrowers of delinquency. Loans in collection are automatically assigned to Dialer Campaigns based on	**A.** Inspected the Collection Department Policies and Procedures to determine whether they exist.	**A.** No deviations noted.
	B. Observed the Dialer operation and inquired with the Dialer Team to determine whether Dialer Campaigns are monitored for completeness daily.	**B.** No deviations noted.

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
loan type (configured during loan setup). Dialer Campaigns are configured to comply with the requirements of the Collections Policy and Procedures. Each day Dialer Campaigns are scheduled for calling. The Dialer Team Supervisor reviews the Dialer daily to determine whether all scheduled collections calls are attempted. Prior to a loan going into foreclosure, the Pre-Foreclosure Manager completes the Pre-Foreclosure Checklist to determine whether the proper notification letters were sent to the borrower.	**C.** Inspected the Pre-Foreclosure checklist for a sample of foreclosed loans during the reporting period to determine whether notification letters are sent to borrowers.	**C.** No deviations noted.
4. The Loss Mitigation Department follows agency and client guidelines to mitigate loss prior to foreclosure. Loss mitigation solicitation notices (also known as early intervention notices) are sent to the borrower.	**A.** Inspected loss mitigation attempts for a sample of loans in foreclosure to determine whether solicitation notices are sent to borrowers.	**A.** No deviations noted.
5. All loans that are placed in foreclosure have had loss mitigation attempts made prior to foreclosure. The Loss Mitigation Checklist is used by the Loss Mitigation Department to ensure loss mitigation is handled according to agency and client guidelines.	**A.** Inspected the Loss Mitigation Checklist for a sample of loans in loss mitigation to determine whether the Loss Mitigation Checklist is used by the Loss Mitigation Department to ensure loss mitigation is handled according to agency and client guidelines.	**A.** No deviations noted.

12. Customer Service and Research

Control Objective: Controls provide reasonable assurance that client concerns are addressed and resolved in a timely manner according to policy, and according to client requirements.

Description of Controls

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
1. Call Center service levels are monitored daily for call answer rate, abandonment rate, and average speed of answer. Call Center performance is reported to Senior Management monthly.	**A.** Inspected service level performance reports and email communications for a sample of months to determine whether Call Center performance is monitored and reported to Senior Management monthly.	**A.** No deviations noted.
2. Call Center Representatives answer private label calls using the client's name and approved greeting.	**A.** Inspected archived calls for a sample of private label clients to determine whether calls are answered with the client's name.	**A.** No deviations noted.
3. On a daily basis, the task reports are emailed to Managers, Assistant Managers, and Supervisors to ensure tasks are completed in a timely manner and according to expected completion dates assigned in the system.	**A.** Inspected task report emails for a sample of days to determine whether the timeliness of task completion is monitored.	**A.** No deviations noted.
4. When a written request for information or error resolution is submitted to DMI, an acknowledgement letter must be sent to the borrower.	**A.** Inspected acknowledgement letters sent to a sample of borrowers to determine whether acknowledgement letters are sent upon written inquiry.	**A.** No deviations noted.
5. Call center performance is evaluated by monitoring eight to ten calls per representative each month by the Customer Service Quality Control Team.	**A.** Inspected quality assurance monitoring forms completed for a sample of customer service representatives and months to determine whether performance is monitored.	**A.** No deviations noted.

13. Data Backup and Recovery

Control Objective: Controls provide reasonable assurance that data and systems are backed up, stored offsite and validated periodically, and operational procedures are documented in sufficient detail to allow the business to continue operations in the event of a short or long term disruption.

Description of Controls

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
1. IT System Administrators are responsible for the backup of data processed in-house. DMI processes differential backups daily and full backups weekly. To monitor for the completion of backup jobs, alerts are sent to the IT Department when backup jobs are not completed successfully.	**A.** Inspected backup schedules to determine whether differential backups are configured to be performed daily and full backups performed weekly.	**A.** No deviations noted.
	B. Inspected the backup alert settings to determine whether alerts are sent to the IT Department when backup jobs are not completed successfully.	**B.** No deviations noted.
2. DMI backup tapes are rotated offsite by the IT System Administrators to a record management company weekly.	**A.** Inspected the Iron Mountain pickup manifests for a sample of weeks to determine whether backup tapes are rotated offsite weekly.	**A.** No deviations noted.
3. Data backup tape restores are performed by the IT System Administrators quarterly.	**A.** Inspected restoration logs for a sample of quarters to determine whether single file restorations are tested quarterly.	**A.** No deviations noted.
4. DMI maintains a Business Continuity Plan which identifies the North Aurora location as the warm-site for the Lake Zurich location and vice versa. In addition, the Plan also identifies SunGard as DMI's vendor for secondary disaster recovery facility.	**A.** Inspected the Business Continuity Plan to determine whether it exists and identifies the warm-site and secondary disaster recovery facility.	**A.** No deviations noted.

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
5. The BCP Committee reviews and documents the BKFS MSP Disaster Recovery test results annually. DMI's ability to set up and restore network servers and workstations, establish connectivity to MSP, process MSP transactions, and establish telecommunications using DMI's toll-free numbers at the secondary disaster recovery site is tested annually and documented in the Operational Disaster Recovery Exercise Report.	**A.** Inspected DMI's documentation of the most recent BKFS MSP Disaster Recovery test results to determine whether DMI reviews the results of BKFS MSP Disaster Recovery test results annually and during the reporting period.	**A.** No deviations noted.
	B. Inspected the Operational Disaster Recovery Exercise Report to determine whether disaster recovery tests are performed annually and during the reporting period.	**B.** No deviations noted.

14. Standard Reporting

Control Objective: Controls provide reasonable assurance that standard reports generated are accurate and complete, and access to modify report templates is restricted.

Description of Controls

Controls Specified by DMI	Testing Performed by Service Auditors	Results of Tests
1. Standard reports are automatically generated based on predefined templates. Accuracy of data is ensured through proper report setup and configuration of the predefined templates.	**A.** Inspected the standard report templates to determine whether standard reports are in place for generation of standard reports.	**A.** No deviations noted.
2. Changes to report templates are governed by the company's change management process and must be authorized by the Development team, tested by an analyst, and approved by a manager or team lead.	**A.** Inspected change tickets for a sample of changes made to report templates to determine whether changes are authorized by the Development team, tested by an analyst, and approved by a manager or team lead.	**A.** No deviations noted.
3. Scheduling of the MSP outputs is performed by IT annually to ensure completeness of outputs. Scheduling performed by IT applies to all clients in the system.	**A.** Inspected evidence of the most recent annual scheduling of MSP outputs that occurred during the reporting period to determine whether IT performed an annual scheduling of the MSP outputs to ensure completeness of outputs.	**A.** No deviations noted.
4. A scheduler is in place to automatically import the MSP outputs to the data warehouse when a new output is detected.	**A.** Inspected the import job scheduler to the data warehouse to determine whether a scheduler is in place to automatically import MSP outputs into the data warehouse when a new output is detected.	**A.** No deviations noted.
5. A scheduler is in place to automatically generate standard reports from the data warehouse.	**A.** Inspected automatic job scheduler settings to determine whether a scheduler is in place to automatically generate standard reports from the data warehouse.	**A.** No deviations noted.

6.	A client table is in place to identify data based on client code and investor code.	**A.**	Inspected the client tables to determine whether client table is in place to identify the client based on client code and investor code.	**A.**	No deviations noted.
7.	Standard reports generated are uploaded in client's FTP folders through an automatic scheduler. The automatic process of report generation ensures the accuracy and completeness of the report content.	**A.**	Inspected the automatic job scheduler settings to determine whether standard report generated are uploaded to client FTP folders based on an automatic scheduler.	**A.**	No deviations noted.
8.	Access to the automatic scheduler, client table, and data warehouse is restricted to authorized users.	**A.**	Inspected a system generated list users with access to the automatic scheduler, client table, and data warehouse to determine whether access is restricted to authorized users.	**A.**	No deviations noted.
9.	The report documents are archived on the client FTP sites for one year in a read only format.	**A.**	Inspected client FTP site settings to determine whether documents are archived for one year in a read-only format.	**A.**	No deviations noted.

plante moran | Audit. Tax. Consulting. Wealth Management.

For more information regarding the report, contact:

Glen S. Braun | Chief Financial Officer
Dovenmuehle Mortgage, Inc.
847.550.7450
glen.braun@dmicorp.com

For more information on Plante Moran, contact:

Timothy R. Bowling, CPA, CCSK, CCSFP | Partner
Plante & Moran, PLLC
312.980.2927
tim.bowling@plantemoran.com