

# Dovenmuehle Mortgage, Inc.

## SOC 2 Type 2 Report

Report on the Subservicing Operations System Relevant to Security, Availability, and Confidentiality Throughout the Period October 1, 2019 to September 30, 2020



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

# Contents

<b>Section 1.</b>	<b>Independent Service Auditor's Report.....</b>	<b>3</b>
<b>Section 2.</b>	<b>Dovenmuehle Mortgage, Inc. Management's Assertion .....</b>	<b>7</b>
<b>Section 3.</b>	<b>Dovenmuehle Mortgage, Inc.'s Description of it Subservicing Operations System Throughout the Period October 1, 2019 to September 30, 2020.....</b>	<b>9</b>
A.	Company Overview .....	9
B.	Scope of the Report .....	9
C.	Principal Service Commitments and System Requirements.....	11
D.	Subservice Organizations .....	12
E.	Company-Level Internal Controls.....	13
F.	Components of the Subservicing Operations System .....	17
G.	Complementary User Entity Controls.....	26
H.	Applicable Trust Service Principles and Related Criteria .....	26
<b>Section 4.</b>	<b>Trust Service Criteria and Dovenmuehle Mortgage, Inc.'s Description of Related Controls and Independent Service Auditor's Description of Test of Controls and Results</b>	<b>27</b>
A.	Common Criteria / Security .....	28
B.	Availability .....	68
C.	Confidentiality .....	73

## 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) accompanying description of its 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) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (AICPA, *Description Criteria*) (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period October 1, 2019 to September 30, 2020, to provide reasonable assurance that DMI's service commitments and system requirements were achieved based on the trust services criteria for security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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 indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at DMI, to achieve DMI's service commitments and system requirements based on the applicable trust services criteria. The description presents DMI's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of DMI's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by 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 complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at DMI, to achieve DMI's service commitments and system requirements based on the applicable trust services criteria. The description presents DMI's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of DMI's controls. Our examination did not include such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such controls.

### **Service organization's responsibilities**

DMI is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that DMI's service commitments and system requirements were achieved. DMI management has provided the accompanying assertion titled "Dovenmuehle Mortgage, Inc. Management's Assertion" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. DMI management is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

### **Service auditor's responsibilities**

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of the controls 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 (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria, and the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion. An examination of the description of a service organization system and the suitability of the design and operating effectiveness of those controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or operating effectively.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

### **Inherent limitations**

The description is prepared to meet the common needs of a broad range of report users and may not, therefore include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature and inherent limitations, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of the controls is subject to the risks that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

### **Description of tests of controls**

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

### **Opinion**

In our opinion, in all material respects,

- a. the description presents DMI's subservicing operations system that was designed and implemented throughout the period October 1, 2019 to September 30, 2020 in accordance with the description criteria.
- b. the controls stated in the description were suitably designed throughout the period October 1, 2019 to September 30, 2020 to provide reasonable assurance that DMI's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of DMI's controls throughout that period.
- c. the controls stated in the description operated effectively throughout the period October 1, 2019 to September 30, 2020 to provide reasonable assurance that DMI's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of DMI's controls operated effectively throughout that period.

## Emphasis of a Matter

As noted in management's description, there were no security incidents during the period October 1, 2019 to September 30, 2020. Therefore, we did not test the operating effectiveness of controls related to Common Criteria 7.4, "The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate," and Common Criteria 7.5, "The entity identifies, develops, and implements activities to recover from identified security incidents," as it relates to implementation of recovery activities.

## 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 DMI, user entities of DMI's subservicing operations system during some or all of the period October 1, 2019 to September 30, 2020, business partners of DMI subject to risks arising from interactions with the system, practitioners providing services to such user entities and business partners, prospective user entities, and business partners and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations and other parties.
- Internal control and its limitations.
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

*Plante & Moran, PLLC*

December 15, 2020



December 15, 2020

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

To Service Auditors:

We have prepared the accompanying 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) based on the criteria DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about DMI's subservicing operations system that may be useful when assessing the risks arising from interactions with the subservicing operations system, particularly information about system controls that DMI has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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 indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at DMI, to achieve DMI's service commitments and system requirements based on the applicable trust services criteria. The description presents DMI's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of DMI's controls. The description does not disclose the actual controls at the subservice organizations.

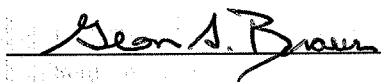
The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at DMI, to achieve DMI's service commitments and system requirements based on the applicable trust services criteria. The description presents DMI's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of DMI's controls.

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

- a. the description presents DMI's subservicing operations system that was designed and implemented throughout the period October 1, 2019 to September 30, 2020 in accordance with the description criteria.
- b. the controls stated in the description were suitably designed throughout the period October 1, 2019 to September 30, 2020 to provide reasonable assurance that DMI's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if subservice organizations and user entities applied the complementary controls assumed in the design of DMI's controls throughout that period.
- c. the controls stated in the description operated effectively throughout the period October 1, 2019 to September 30, 2020 to provide reasonable assurance that DMI's service commitments and system requirements would be achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of DMI's controls operated effectively throughout that period.

As noted in management's description, there were no incidents during the period October 1, 2019 to September 30, 2020. Therefore, controls related to Common Criteria 7.4, "The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate," and Common Criteria 7.5, "The entity identifies, develops, and implements activities to recover from identified security incidents." did not operate during the period October 1, 2019 to September 30, 2020.

Very truly yours,



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

---

The scope of this report is limited to DMI's subservicing operations system throughout the period October 1, 2019 to September 30, 2020 based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, Description Criteria) (description criteria), and the controls to achieve DMI's service commitments and system requirements based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria) specific to DMI's Lake Zurich, Elgin, and North Aurora facilities.

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. Principal Service Commitments and System Requirements

DMI makes service commitments to its customers and has established system requirements as part of the subservicing operations system. Some of these commitments are principal to the performance of the service and relate to applicable trust services criteria. DMI is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that DMI's service commitments and system requirements are achieved.

A description of the service offering and the service commitments to customers are documented and communicated in the Subservicing Agreement. DMI's principal service commitments are:

- **Security** – DMI shall have and maintain measures in place as reasonably appropriate to provide physical, electronic, and procedural safeguards for the use, maintenance, and disclosure of data in accordance with applicable requirements. DMI agrees to maintain policies and procedures to promptly and adequately address any incidents of unauthorized access, misuse or disclosure of confidential information by its authorized recipients.
- **Availability** – DMI shall maintain a business continuity and disaster recovery plan in compliance with applicable requirements. DMI shall test the plan at least annually. The plan shall provide for an alternative site that can be operational, and from which services detailed in the subservicing agreement can be performed, within two business days following the declaration of a disaster by DMI's senior management. DMI shall coordinate with the lender in setting up all telecommunication modifications that might be necessary for the lender to achieve connectivity to DMI's alternate site and, during any period for which the alternative site is in use, DMI shall provide status updates to the lender as is appropriate under the circumstances.
- **Confidentiality** – DMI shall maintain strict confidentiality of client, borrower, and employee information. All business relationships are covered by agreements such as Non-Disclosure and Confidentiality Agreements. DMI is aware of and complies with all applicable state and federal rules and regulations surrounding privacy and confidentiality of information.

DMI has established operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated through the company's policies and procedures and agreements with customers. Policies and procedures define an organization-wide approach to how systems and data are protected. These include policies around how the system is designed and operated, how the network and systems are managed and how employees are hired and trained. Principle system requirements are:

- Implementing reasonable internal control to address significant risk
- Designing the system to prevent unauthorized access
- Monitoring system alerts for security, availability, and confidentiality incidents
- Escalating security, availability, and confidentiality events based upon its policies and procedures defined in its Incident Response Plan
- Managing application and infrastructure changes

## D. 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 service commitments and system requirements would be achieved. These complementary subservice organization controls and the related trust services criteria 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 trust services criteria that are applicable to the services that they provide:

- **Black Knight Financial Services, Inc. (BKFS)** - Mortgage Servicing Platform (MSP) for computer 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.
- **Iron Mountain Information Management, LLC (Iron Mountain)** - offsite media archival
- **TM Systems Pvt. Ltd (TM Systems)** - offsite data entry
- **SunGard Availability Services LP (SunGard)** - disaster recovery site

Applicable Trust Services Criteria	Expected Controls to be Implemented by the Subservice Organization
Common Criteria 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The following controls are applicable to BKFS and TM Systems:  Users must authenticate to the network and applications.  Administrative access to the network and applications are restricted.
Common Criteria 6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The following controls are applicable to BKFS, Iron Mountain, TM Systems, and SunGard:  All entrances to the building and data center are locked and access is properly restricted.  A user access review of individuals with access to the data center is reviewed.

<p>Common Criteria 7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.</p> <p>Common Criteria 7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.</p>	<p>The following are controls expected to be present at BKFS and TM Systems:</p> <p>Firewall and IDS are in place and properly monitored.</p> <p>Scheduled backups are monitored for completeness.</p>
<p>Common Criteria 7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.</p> <p>Common Criteria 7.4: The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.</p>	<p>The following controls are applicable to BKFS, Iron Mountain, TM Systems, and SunGard:</p> <p>Incident management policies and procedures are defined and implemented for incident handling and breach management.</p>
<p>Common Criteria 8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.</p>	<p>The following controls are applicable to BKFS:</p> <p>A change management process is in place.</p>

## E. 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.

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. The Incident Response Plan outlines the procedures to report incidents and is made readily available to employees on the internal document management portal. Security Awareness Training is provided to employees upon hire and on an annual basis to ensure the ISP is effectively communicated to employees.

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. A Risk Assessment Guide is formally documented and defines the scope, frequency, objectives, and procedures for the identification and assessment of risks related to the achievement of system objectives. The risk assessment process measures business process risk and information system risk.

During the risk assessment process, management evaluates the fraud risks related to the use of IT and access to information. As part of the risk assessment, management evaluates how information is collected and where to collect information from in order to evaluate whether internal controls are operating as expected. The Risk Assessment is complete with respect to linking controls with risks that threaten the achievement of business process and IT control objectives. A mix of controls types (i.e. preventative, detective, automatic, or manual) are identified to address the various risks. Segregation of duties exist in logical access and change management functions.

Quarterly Information Security Officer Committee meetings are held to evaluate risks related to security, availability, and confidentiality. The Compliance Committee meets on a monthly basis to discuss regulatory changes or issues that were identified.

An Information Security and System Risk Assessment is conducted annually. The risk assessment is reviewed and approved by the Board of Directors to ensure DMI acts to mitigate risks.

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 DMICConnect 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 DMICConnect. The Subservicing Policy Manual is provided to clients at the time of boarding. 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. 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 preventative, detective, automatic, and manual controls to manage risks.

## F. 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 imaging 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.

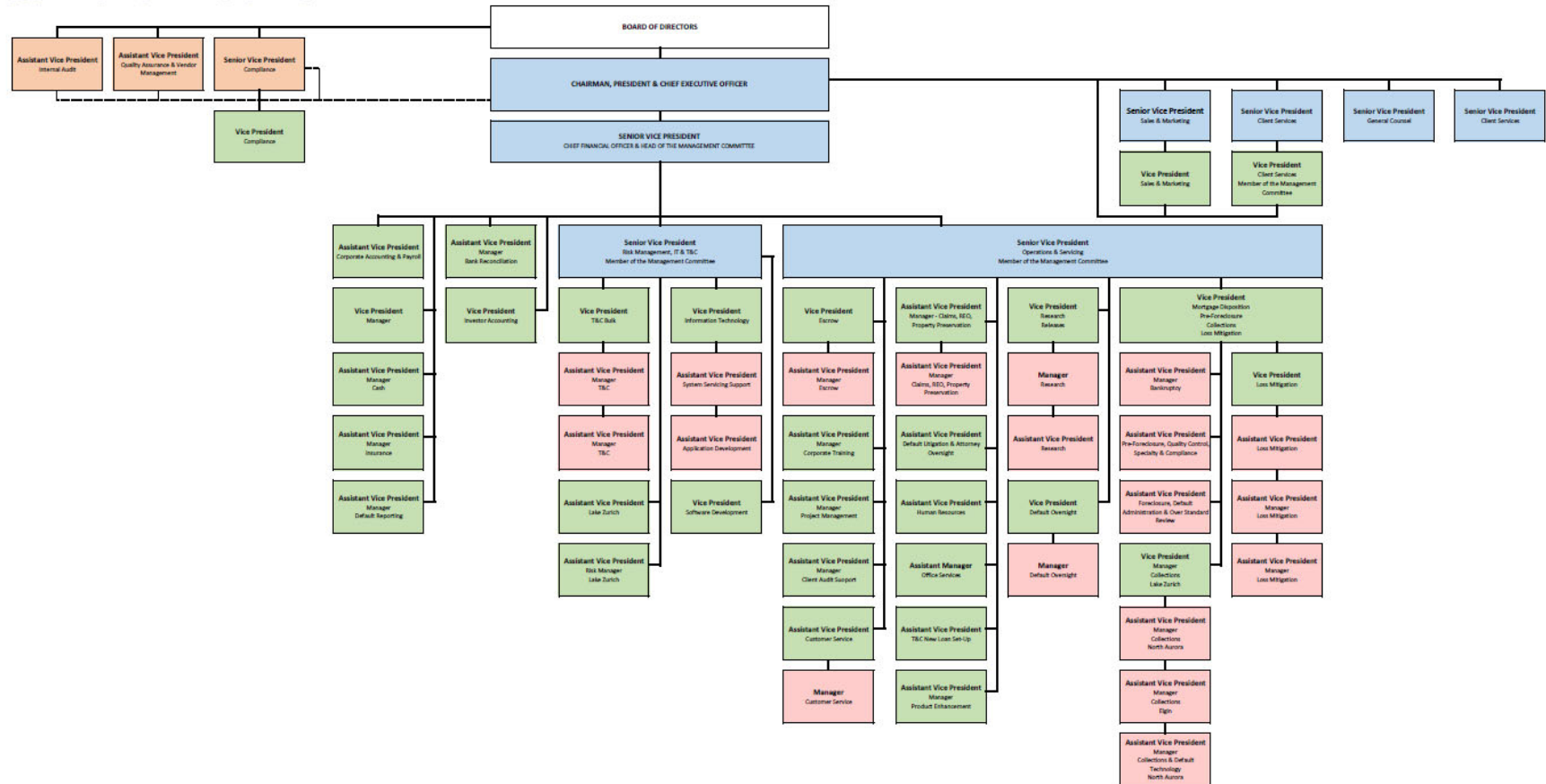
DMI provides clients with online access to corporate and loan level documents through the DMISConnect system. Items such as policies, procedures, due diligence documents, servicing documents, newsletters, and client announcements are accessible. This system provides clients access to other DMI products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



## 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 a key card 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 1 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.

### **Environment 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 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 when new accounts are created. One includes the Remote Inquiry System (RIS) Client Manual, the second consists of the username, and the third indicates the end-user's password. Access restrictions for the client portal (DMISConnect) include the following: 1) 8 characters minimum, including letters and numbers, 2) lockout after 20 min of inactivity, 3) lockout after 5 failed login attempts, and 4) passwords expire after 90 days.

Access restrictions for Silver borrower websites include the following: 1) usernames must consist of at least 5 characters, including letters and numbers and 2) passwords must have at least 10 characters, including one uppercase, one lowercase, and one number.

Access restrictions for Gold borrower websites (non-SSO) include the following: 1) access is device and location-specific; users are sent confirmation code to verify the user if signing in from new device or new location, 2) borrowers must provide loan #, last four digits of social security number, and property zip code, then confirm the account via email (expires after 72 hours) in order to set up account on website, and 3) maximum of one borrower per loan.

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.

When an employee is terminated, IT evaluates whether the workstation will be decommissioned, reimaged, or kept on the floor. Workstations to be decommissioned are noted within the termination help desk ticket and tracked to completion. Workstations to be decommissioned or reimaged are locked and maintained by the IT department. Disposal of assets are tracked to ensure assets are sanitized prior to disposal.

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.

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. Vulnerability scans are performed by the IT Team monthly and critical/high risk findings are remediated. A third party penetration test is performed annually and critical/high risk findings are remediated.

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.

---

## G. 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 service commitments and system requirements would be achieved. These complementary user entity controls and the related trust services criteria are described below. User entities are responsible for implementing such controls.

- User entities are responsible for protecting login credentials to DMI systems. (Common Criteria 6.1)
- User entities are responsible for timely logging out of terminals to protect their proprietary data. (Common Criteria 6.1)
- User entities are responsible for notifying DMI personnel in the event that an incident related to security and confidentiality is encountered during use of the system. (Common Criteria 7.3)

## H. Applicable Trust Service Principles and Related Criteria

---

The organization's applicable trust services criteria and the related controls designed to meet those criteria, 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 applicable trust services criteria and related controls are presented in Section 4, they are an integral part of DMI's description of system.

---

## Section 4. Trust Service Criteria and Dovenmuehle Mortgage, Inc.'s Description of Related Controls and Independent Service Auditor's Description of Test of Controls and Results

This section presents the following information provided by DMI:

- The applicable trust services criteria specified by the management of DMI
- The controls established and specified by DMI to achieve the specified service commitments and system requirements based on the applicable trust services criteria.

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 service commitments and system requirements were achieved based on the applicable trust services criteria. 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.

## A. Common Criteria / Security

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
<b>1.0 Common Criteria related to Control Environment</b>			
<b>1.1</b> The entity demonstrates a commitment to integrity and ethical values.			
	1. The Employee Handbook contains disciplinary actions to take against employees whose behaviors deviate from the company's expected standards of conduct, which include integrity and ethics.	Inspected the Employee Handbook to determine whether it outlines disciplinary actions to take against employees whose behaviors deviate from the company's expected standards of conduct.	No deviations noted.
	2. 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.	Inspected employee handbook acknowledgement forms for a sample of new hires to determine whether employees are required to read and acknowledge the handbook.	No deviations noted.
	3. Annual performance reviews are performed and documented with a checklist that is signed by the employee and the manager.	Inspected the annual performance review checklist for a sample of employees to determine whether annual performance reviews are performed and documented with a checklist that is signed by the employee and the manager.	No deviations noted.

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
<b>1.2</b> The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	<b>1.</b> 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.	Inspected the meeting minutes for a sample of quarters to determine whether the Board of Directors includes members who are independent from management and meets at least quarterly to discuss the business operations and monitor internal control operations.	No deviations noted.
	<b>2.</b> The risk assessment is reviewed and approved annually by the Board of Directors to ensure DMI acts to mitigate risks.	Inspected Board of Directors meeting minutes to determine whether the risk assessment is reviewed and approved annually by the Board of Directors during the reporting period.	No deviations noted.
<b>1.3</b> Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	<b>1.</b> 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.	Inspected the DMI organization chart to determine whether management oversight functions are segregated.	No deviations noted.
		Inspected the company's intranet to determine whether the organization chart is made available to employees through the company's intranet.	No deviations noted.
	<b>2.</b> Job descriptions are documented and specify the roles and responsibilities of internal users.	Inspected job descriptions for a sample of users to determine whether job descriptions are formally documented.	No deviations noted.

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
	3. 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.	Inspected the ISP to determine whether the responsibilities for security, confidentiality, and availability are documented.	No deviations noted.
1.4 The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
	1. Candidates are evaluated by HR and managers or supervisor as part of the new hire processes.	Inspected the candidate cover sheets for a sample of new hires to determine whether candidates are evaluated as part of the onboarding process.	No deviations noted.
	2. Background checks are performed by HR on every DMI employee upon hiring. Background checks cover federal and state violations and financial history.	Inspected background check reports for a sample of new hires to determine whether background checks are performed for all employees upon hire.	No deviations noted.
	3. Security Awareness Training is provided to employees upon hire and on an annual basis to ensure the ISP is effectively communicated to employees.	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 and during the reporting period.	<b>Deviations noted.</b> Annual security awareness training was not completed during the reporting period for 4 of 20 employees selected for testing.
		Inspected Security Awareness Training completion forms for a sample of new hires to determine whether Security Awareness Training is provided to employees upon hire.	No deviations noted.

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
	4. Annual performance reviews are performed and documented with a checklist that is signed by the employee and the manager.	Inspected the annual performance review checklist for a sample of employees to determine whether annual performance reviews are performed during the reporting period and documented with a checklist that is signed by the employee and the manager.	No deviations noted.
1.5 The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
	1. Annual performance reviews are performed and documented with a checklist that is signed by the employee and the manager.	Inspected the annual performance review checklist for a sample of employees to determine whether annual performance reviews are performed during the reporting period and documented with a checklist that is signed by the employee and the manager.	No deviations noted.
	2. The Employee Handbook contains disciplinary actions to take against employees whose behaviors deviate from the company's expected standards of conduct, which includes integrity and ethics.	Inspected the Employee Handbook to determine whether it outlines disciplinary actions to take against employees whose behaviors deviate from the company's expected standards of conduct.	No deviations noted.

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
	3. Performance metrics are established for individuals with significant internal control responsibilities, which are evaluated by the employee's manager or supervisor as part of the annual performance reviews.	Inspected performance reviews for a sample of individuals with significant internal control responsibilities to determine whether performance reviews are performed annually during the reporting period to hold individuals with significant internal control responsibilities accountable.	No deviations noted.

## 2.0 Common Criteria related to Communication and Information

### 2.1 The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.

1. As part of the risk assessment, management evaluates how information is collected and where to collect information from in order to evaluate whether internal controls are operating as expected.	Inspected the most recent Information Security and System Risk Assessment to determine whether management evaluates how information is collected and where to collect information from as part of the risk assessment.	No deviations noted.
2. The Quality Assurance Plans document auditing plans ranging across different business departments to assess the adequacy and effectiveness of controls in place.	Inspected the Quality Assurance Plans to determine whether the Quality Assurance Plans are documented and outline auditing plans ranging across different business departments to assess the adequacy and effectiveness of controls in place.	No deviations noted.



Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
<b>2.2</b> The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
	1. 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.	Inspected employee handbook acknowledgement forms for a sample of new hires to determine whether employees are required to read and acknowledge the handbook.	No deviations noted.
	2. All policies and procedures, including the ISP, are available to all employees on the internal document management portal.	Inspected the internal document management portal to determine whether policies and procedures, including ISP, are made available to all employees.	No deviations noted.
	3. All DMI employees are required to sign a confidentiality form at the time of hire stating that they will keep all client information, all mortgagor information, and any other private information strictly confidential.	Inspected signed confidentiality agreements for a sample of new hires to determine whether employees are required to acknowledge and sign confidentially agreements at the time of hire.	No deviations noted.
	4. Security Awareness Training is provided to employees upon hire and on an annual basis to ensure the ISP is effectively communicated to employees.	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 and during the reporting period.	<b>Deviations noted.</b> Annual security awareness training was not completed during the reporting period for 4 of 20 employees selected for testing.

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
		Inspected Security Awareness Training completion forms for a sample of new hires to determine whether Security Awareness Training is provided to employees upon hire.	No deviations noted.
	5. The Incident Response Plan outlines the procedures to report incidents and is made readily available to employees on the internal document management portal.	Inspected the Incident Response Plan to determine whether it communicates how employees should follow the IRP to report incidents.	No deviations noted.
		Inspected the internal document management portal to determine whether the Incident Response Plan is readily available to employees.	No deviations noted.
	6. 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.	Inspected notifications sent for a sample of changes that affected internal or external users to determine changes are evaluated and communicated to internal and external parties.	No deviations noted.
	7. Any updates to confidentiality policies are communicated internally via email or incorporated into the annual security awareness training. Updates are	Inquired with management to obtain an understanding of the process for communicating updates to confidentiality policies for internal and external users.	No deviations noted.

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
	<p>communicated externally by Account Managers via the All Points Bulletin (APB) email.</p> <p>There were no updates to the confidentiality policies made during the period. Therefore, there was no circumstance that warranted the performance of the control.</p>	<p>Inspected the current and prior year confidentiality practices and inquired with the Legal Counsel to verify that there were no updates to the confidentiality policies within the reporting period.</p>	<p>Not applicable. There was no circumstance that warranted the performance of the control. Accordingly, no testing was performed by us.</p>
<b>2.3</b> The entity communicates with external parties regarding matters affecting the functioning of internal control.			
	<p><b>1.</b> The Subservicing Policy Manual describes all services and boundaries of the system to clients, and is provided to clients at the time of onboarding.</p> <p>Updates to the manual are provided to clients through DMICConnect.</p>	<p>Inspected the most recent Subservicing Policy Manual to determine whether it describes all services and boundaries of the system to clients.</p> <p>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.</p> <p>Inspected the DMICConnect site to determine whether updated versions of the manual are provided to clients through DMICConnect.</p>	<p>No deviations noted.</p> <p>No deviations noted.</p> <p>No deviations noted.</p>
	<p><b>2.</b> Specific services provided to each client are defined in signed Subservicing Agreements. Security, availability, and confidentiality commitments are communicated to clients via Subservicing Agreements.</p>	<p>Inspected the Subservicing Agreements for a sample of new clients to determine whether security, availability, and confidentiality commitments are communicated to clients.</p>	<p>No deviations noted.</p>

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
	3. The Subservicing Policy Manual and DMICConnect Client Administrator Guide inform clients how to report any issues.	Inspected the Subservicing Policy Manual and DMICConnect Client Administrator Guide to determine whether it provides clients information about how to report any issues.	No deviations noted.
	4. DMI websites list contact information. Standard Billing statements contain appropriate DMI contact information for borrowers in the event of questions or concerns.	Inspected the DMI website and Standard Billing Statements to determine whether DMI contact information is provided.	No deviations noted.
	5. 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.	Inspected notifications sent for a sample of changes that affected internal or external users to determine changes are evaluated and communicated to internal and external parties.	No deviations noted.
	6. Any updates to confidentiality policies are communicated internally via email or incorporated into the annual security awareness training. Updates are communicated externally by Account Managers via the All Points Bulletin (APB) email.	Inquired with management to obtain an understanding of the process for communicating updates to confidentiality policies for internal and external users.	No deviations noted.
	There were no updates to the confidentiality policies made during the period. Therefore, there was no circumstance that warranted the performance of the control.	Inspected the current and prior year confidentiality practices and inquired with the Legal Counsel to verify that there were no updates to the confidentiality policies within the reporting period.	Not applicable. There was no circumstance that warranted the performance of the control. Accordingly, no testing was performed by us.

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
<b>3.0 Common Criteria related to Risk Assessment</b>			
<b>3.1</b> The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
	<b>1.</b> A Risk Assessment Guide is formally documented and defines the scope, frequency, objectives, and procedures for the identification and assessment of risks related to the achievement of system objectives. Risk assessment methodology is specified in the Risk Assessment Guide to enable a complete and accurate identification of objectives.	Inspected the Risk Assessment Guide to determine whether it is formally documented and defines the scope, frequency, objectives, and procedures for the identification and assessment of risks related to the achievement of system objectives.	No deviations noted.
		Inspected the Risk Assessment Guide to determine whether the risk assessment methodology is specified in the Risk Assessment Guide to enable a complete and accurate identification of objectives.	No deviations noted.
	<b>2.</b> The Information Security and System Risk Assessment identifies and ranks information assets according to sensitivity, which is used to determine risk impact.	Inspected the most recent Information Security and System Risk Assessment to determine whether DMI has a process to identify and rank its information assets according to sensitivity, and whether the sensitivity ranking is used in the determination of risk impact.	No deviations noted.

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
<b>3.2</b> The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
	1. An enterprise-wide risk assessment representing all areas of the organization and an Information Security and System Risk Assessment are conducted annually by the Information Security Officer Committee.	Inspected the most recent Enterprise-Wide Risk Assessment and the Information Security and System Risk Assessment to determine whether they are conducted annually by the Information Security Officer Committee .	No deviations noted.
	2. The risk assessment is reviewed and approved annually by the Board of Directors to ensure DMI acts to mitigate risks.	Inspected Board of Directors minutes to determine whether the risk assessment is reviewed and approved annually by the Board of Directors during the reporting period.	No deviations noted.
	3. Quarterly Information Security Officer Committee meetings are held to evaluate risks related to security, availability, and confidentiality.	Inspected the Information Security Officer Committee meeting minutes for a sample of quarters to determine whether quarterly Information Security Officer Committee meetings are held to evaluate risks related to security, availability, and confidentiality.	No deviations noted.
	4. An ITGC review is performed by the Internal Audit Department on a quarterly basis. The ITGC review enables the company to monitor ITGCs and provide relevant information for the risk assessment process.	Inspected the ITGC review results for a sample of quarters to determine whether an ITGC review is performed by the Internal Audit Department on a quarterly basis to monitor ITGCs and provide relevant information for the risk assessment process.	No deviations noted.

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
<b>3.3</b> The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
	1. During the risk assessment process, management evaluates the fraud risks related to the use of IT and access to information.	Inspected the most recent Information Security and System Risk Assessment to determine whether fraud risks are considered.	No deviations noted.
<b>3.4</b> The entity identifies and assesses changes that could significantly impact the system of internal control.			
	1. The Compliance Committee meets on a monthly basis to discuss regulatory changes or issues that were identified.	Inspected Compliance Committee meeting minutes for a sample of months to determine whether the Compliance Committee meets on a monthly basis to discuss regulatory changes or issues that were identified.	No deviations noted.
	2. Quarterly Information Security Officer Committee meetings are held to evaluate risks related to security, availability, and confidentiality.	Inspected the Information Security Officer Committee meeting minutes for a sample of quarters to determine whether quarterly Information Security Officer Committee meetings are held to evaluate risks related to security, availability, and confidentiality.	No deviations noted.
	3. Any changes required as a result of the risk assessment are tracked by the IT Steering Committee for completion.	Inspected the Information Technology Steering Committee Meeting minutes to determine whether changes from the risk assessment are tracked for completion.	No deviations noted. 100% of the population was tested.

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
	4. 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.	Inspected notifications sent for a sample of changes that affected internal or external users to determine changes are evaluated and communicated to internal and external parties.	No deviations noted.

#### 4.0 Common Criteria related to Monitoring Activities

4.1 The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

1. The Quality Assurance Plans document auditing plans ranging across different business departments to assess the adequacy and effectiveness of controls in place.	Inspected the Quality Assurance Plans to determine whether the Quality Assurance Plans are documented and outline auditing plans ranging across different business departments to assess the adequacy and effectiveness of controls in place.	No deviations noted.
2. An ITGC review is performed by the Internal Audit Department on a quarterly basis. The ITGC review enables the company to monitor ITGCs and provide relevant information for the risk assessment process.	Inspected the ITGC review results for a sample of quarters to determine whether an ITGC review is performed by the Internal Audit Department on a quarterly basis to monitor ITGCs and provide relevant information for the risk assessment process.	No deviations noted.
3. A third party penetration test is performed annually and corrective actions are performed for any high or critical findings.	Inspected the results of the most recent third party penetration test to determine whether penetration testing is performed annually and corrective actions are performed for any high or critical findings.	No deviations noted.



Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
	4. Third party penetration tests are performed on borrower websites at least annually and corrective actions are performed for any high or critical findings.	Inspected the results of third party penetration test on borrower websites to determine whether penetration testing is performed annually and during the reporting period and corrective actions are performed for any high or critical findings.	No deviations noted.
	5. Firewall, workstation, and database hardening guidelines are in place and reviewed annually by the VP of IT.	Inspected the firewall, workstation and database hardening guidelines to determine whether they are formally documented and reviewed annually.	No deviations noted.
<b>4.2</b> The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
	1. 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.	Inspected notifications sent for a sample of changes that affected internal or external users to determine changes are evaluated and communicated to internal and external parties.	No deviations noted.
	2. Control deficiencies identified in performing control monitoring result in corrective action plans.	Inspected control assessment results to determine whether deficiencies are identified and corrective action plans are taken.	No deviations noted.
	3. The results of internal controls monitoring are reported to the Board of Directors at least annually.	Inspected Board of Directors meeting minutes to determine whether the results of internal controls monitoring are reported to the board at least annually and during the reporting period.	No deviations noted.

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
<b>5.0 Common Criteria related to Control Activities</b>			
<b>5.1</b> The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
	1. The Risk Assessment is complete with respect to linking controls with risks that threaten the achievement of business process and IT control objectives. A mix of controls types (i.e. preventative, detective, automatic, or manual) are identified to address the various risks.	Inspected the most recent Information Security and System Risk Assessment to determine whether controls address business process and IT risks, and whether a mix of control types is used to respond to risk.	No deviations noted.
	2. The Enterprise-Wide Risk Assessment and the Information Security and System Risk Assessment outlines the segregation of duties implemented for logical access and change management functions.	Inspected the most recent Enterprise-Wide Risk Assessment and the Information Security and System Risk Assessment to determine whether segregation of duties is implemented in high risk areas such as logical access and change management.	No deviations noted.
<b>5.2</b> The entity also selects and develops general control activities over technology to support the achievement of objectives.			
	1. The Risk Assessment is complete with respect to linking controls with risks that threaten the achievement of business process and IT control objectives. A mix of controls types (i.e. preventative, detective, automatic, or manual) are identified to address the various risks.	Inspected the most recent Information Security and System Risk Assessment to determine whether controls address business process and IT risks, and whether a mix of control types is used to respond to risk.	No deviations noted.

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
<b>5.3</b> The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
	1. An Information Security Policy (ISP) is developed based on the risk assessment and controls that documents employee responsibilities for the use of DMI technology, programs, files, unauthorized use of passwords, and the appropriate use of the Internet.	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.	No deviations noted.
	2. Each DMI department that performs mortgage subservicing activities has written standards and procedures documents, and reviews them on an annual basis. The documents are made available to employees through the company's internal document management portal.	Inspected standards and procedures documents for a sample of departments to determine whether the documents that describe departmental procedures exist and are reviewed annually and during the reporting period.	No deviations noted.
		Inspected the internal document management portal to determine whether standards and procedures documents are made available to all employees.	No deviations noted.
	3. 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.	Inspected the SDLC policy to determine whether it is formally documented and reviewed annually by the IT team.	No deviations noted.

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
	4. The Quality Assurance Plans document auditing plans ranging across different business departments to assess the adequacy and effectiveness of controls in place.	Inspected the Quality Assurance Plans to determine whether the Quality Assurance Plans are documented and outline auditing plans ranging across different business departments to assess the adequacy and effectiveness of controls in place.	No deviations noted.
<b>6.0 Common Criteria related to Logical and Physical Access Controls</b>			
<b>6.1</b> The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
	1. A username and password is required to access the client portals.	Observed an attempt to access the client portals to determine whether a username and password is required.	No deviations noted.
	2. 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.	Inspected user access requests for a sample of new clients to determine whether user accounts are authorized by the client.	No deviations noted.
		Inspected system configurations to determine whether clients are restricted from accessing information of other clients in MSP.	No deviations noted.
	3. Client's IP address ranges are hardcoded in the firewall rule set to explicitly allow traffic only from preauthorized sources.	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.	No deviations noted.

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
	<b>4.</b> Authentication parameters to the SFTP include the following: <ul style="list-style-type: none"> <li>- users are identified with certificates stored on their workstations</li> <li>- accounts are disabled after 68 days of inactivity and deleted after 365 days after being disabled</li> </ul>	Inspected the SFTP authentication parameters to determine whether they are in accordance with the control stated.	No deviations noted.
	<b>5.</b> Access restrictions for the client portal (DMICConnect) include the following: <ul style="list-style-type: none"> <li>- 8 characters minimum, including letters and numbers</li> <li>- lockout after 20 min of inactivity</li> <li>- lockout after 5 failed login attempts</li> <li>- passwords expire after 90 days</li> </ul>	Inspected the DMICConnect authentication parameters to determine whether they are in accordance with the control stated.	No deviations noted.
	<b>6.</b> Access restrictions for Silver borrower websites include the following: <ul style="list-style-type: none"> <li>- Usernames must consist of at least 5 characters, including letters and numbers</li> <li>- Passwords must have at least 10 characters, including one uppercase, one lowercase, and one number</li> </ul>	Inspected the Silver borrower website authentication parameters to determine whether they are in accordance with the control stated.	No deviations noted.

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
	<p><b>7.</b> Access restrictions for Gold borrower websites include the following:</p> <ul style="list-style-type: none"> <li>- access is device and location-specific; users are sent confirmation code to verify the user if signing in from new device or new location</li> <li>- borrowers must provide loan #, last four digits of social security number, and property zip code, then confirm the account via email (expires after 72 hours) in order to set up account on website</li> <li>- maximum of one borrower per loan</li> </ul>	Inspected the Gold borrower website authentication parameters to determine whether they are in accordance with the control stated.	No deviations noted.
	<p><b>8.</b> 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 15 minutes of inactivity.</p>	Inspected the LAN authentication parameters to determine whether LAN password parameters are configured as stated in the control description.	No deviations noted.
	<p><b>9.</b> 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.</p>	Inspected the MSP authentication standards to determine whether MSP password parameters are configured as stated in the control description.	No deviations noted.
	<p><b>10.</b> Passwords for borrower websites are stored hashed.</p>	Inspected the password hash settings to determine whether passwords are stored hashed.	No deviations noted.

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
	<b>11.</b> Local administration access is restricted to prevent users from installing software. The ability to install software is limited to authorized administrators.	Inspected the system configurations to determine whether the ability to install software is restricted from local users.	No deviations noted.
	<b>12.</b> DMI network administrative access is limited to members of the Systems Department that require that level of access to perform their job duties.	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.	No deviations noted.
	<b>13.</b> Administrator level access to the MSP system is limited to only those authorized individuals requiring that level of access to perform their job duties.	Inspected a system generated list of users with MSP administrative access to determine whether access is restricted to authorized users based on job functions.	No deviations noted.
	<b>14.</b> Access to make changes to the firewall is restricted to network administrators.	Inspected a system generated list of firewall administrators to determine whether access is restricted to network administrators.	No deviations noted.
	<b>15.</b> Access to the production environment is restricted to authorized users.	Inspected a system-generated list of users with access to the production environment to determine whether access to the production environment is limited to authorized users.	No deviations noted.

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
<b>6.2</b> Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
	1. New hire access requests are performed using a completed security request form. Department managers must complete and approve the form. Requests are processed by the Technology Department.	Inspected access request forms for a sample of new hires to determine whether access is authorized by a manager.	No deviations noted.
		Inspected access provisioned for a sample of new hires to determine whether access is provisioned by the Technology Department as requested.	No deviations noted.
	2. Employees are only granted VPN access if approved by their department manager in a security request form.	Inspected access request forms for a sample of users granted VPN access during the period to determine whether access is authorized by the department managers.	No deviations noted.
	3. Client access to DMICConnect is managed by clients, except access to the Remote Inquiry System (RIS). RIS access requires client approval and is granted by the DMI Helpdesk.	Inspected access requests for a sample of new RIS users to determine whether access is authorized by the client.	No deviations noted.
	4. A daily report is generated for all changes made to MSP accounts. The IT Security and Compliance Team reviews the reports daily.	Inspected MSP access change reports for a sample of days to determine whether the IT Security and Compliance Team reviews the reports on a daily basis.	No deviations noted.



Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
	<p>5. The Systems Department is notified of employee terminations at the time of termination through the help desk system and access is revoked by IT Helpdesk within two business days.</p>	<p>Inspected the termination requests for a sample of terminated employees to determine whether the Systems Department is notified of the terminations.</p>	No deviations noted.
	<p>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.</p>	<p>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.</p>	No deviations noted.
	<p>6. When a client agreement is transferred out and client access is no longer necessary, clients notify the account manager. Client IP addresses are removed by the System Administrators and all client accounts are deleted by the IT Helpdesk within 90 days of the loan transfer date.</p>	<p>Inspected the service release help desk tickets for a sample of clients that have transferred out to determine whether access is removed timely.</p>	No deviations noted.
<p>6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.</p>			
	<p>1. New hire access requests are performed using a completed security request form. Department managers must complete and</p>	<p>Inspected access request forms for a sample of new hires to determine whether access is authorized by a manager.</p>	No deviations noted.

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
	approve the form. Requests are processed by the Technology Department.	Inspected access provisioned for a sample of new hires to determine whether access is provisioned by the Technology Department as requested.	No deviations noted.
	2. Employees are only granted VPN access if approved by their department manager in a security request form.	Inspected access request forms for a sample of users granted VPN access during the period to determine whether access is authorized by the department managers.	No deviations noted.
	3. The Systems Department is notified of employee terminations at the time of termination through the help desk system and access is revoked by IT Helpdesk within two business days.	Inspected the termination requests for a sample of terminated employees to determine whether the Systems Department is notified of the terminations.	No deviations noted.
	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.	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.	No deviations noted.
	4. 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.	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.	No deviations noted.

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
	5. Client access to DMICConnect is managed by clients, except access to the Remote Inquiry System (RIS). RIS access requires client approval and is granted by the DMI Helpdesk.	Inspected access requests for a sample of new RIS users to determine whether access is authorized by the client.	No deviations noted.
	6. A daily report is generated for all changes made to MSP accounts. The IT Security and Compliance Team reviews the reports daily.	Inspected MSP access change reports for a sample of days to determine whether the IT Security and Compliance Team reviews the reports on a daily basis.	No deviations noted.
	7. When a client agreement is transferred out and client access is no longer necessary, clients notify the account manager. Client IP addresses are removed by the System Administrators and all client accounts are deleted by the IT Helpdesk within 90 days of the loan transfer date.	Inspected the service release help desk tickets for a sample of clients that have transferred out to determine whether access is removed timely.	No deviations noted.
<b>6.4</b> The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
	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.	Observed the Lake Zurich, North Aurora, and Elgin buildings to determine whether access to the DMI office suites is controlled by electronic key cards.	No deviations noted.

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
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.	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.	No deviations noted.
	Similarly, visitors to the Elgin facility must sign the visitors' log and be escorted by a DMI employee.	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.	No deviations noted.
	Visitors to the North Aurora facility must be escorted by a DMI employee at all times.	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.	No deviations noted.
	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.		
3.	Access cards and access levels are granted based upon an Access Card Request form that is submitted by DMI.	Inspected the Access Card Request form for a sample of new hires to determine whether badge access is authorized.	No deviations noted.
4.	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.	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.	No deviations noted.

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
	5. The HR department conducts a quarterly review of access levels to the building and suite for all three office locations.	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.	No deviations noted.
	6. 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.	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.	No deviations noted.
	Access is restricted to members of the Information Technology Department and Executive Management.	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.	No deviations noted.
	7. Physical access to the SunGard disaster recovery site is restricted to authorized individuals. Physical controls at the disaster recovery site are managed by SunGard.	Inspected a system-generated list of individuals with access to the SunGard disaster recovery site to determine whether access is restricted to authorized individuals.	No deviations noted.

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
	<b>8.</b> The authority to request and receive backup tapes is restricted to authorized individuals. Physical controls at the offsite tape storage facility are managed by Iron Mountain.	Inspected a system-generated list of individuals with the authority to request and receive backup tapes to determine whether the authority is restricted to authorized individuals.	No deviations noted.
	<b>9.</b> Individuals with access to the SunGard disaster recovery site and Iron Mountain are reviewed annually by the IT Security Compliance Analyst.	Inspected the most recent SunGard and Iron Mountain access reviews to determine whether it is performed annually by the IT Security Compliance Analyst.	No deviations noted.
	<b>10.</b> Backup tapes are stored in the onsite Lake Zurich data center and access is restricted to authorized personnel.	Observed the onsite data center to determine whether backups tapes are stored in the onsite data center and access to the data center is restricted.	No deviations noted.
		Inspected a system generated list of individuals with access to the Lake Zurich data center to determine whether access is restricted to authorized personnel.	No deviations noted.

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
	<p><b>11.</b> 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.</p> <p>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.</p>	Inspected termination checklists for a sample of terminated employees to determine whether access is revoked upon termination within one business day.	No deviations noted.
<b>6.5</b> The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
	<p><b>1.</b> When an employee is terminated, IT evaluates whether the workstation will be decommissioned, reimaged, or kept on the floor. Workstations to be decommissioned are noted within the termination help desk ticket and tracked to completion.</p> <p>Workstations to be decommissioned or reimaged are locked and maintained by the IT department.</p>	<p>Inspected the termination help desk tickets for a sample of terminated employees to determine whether workstations for terminated employees are decommissioned or reimaged.</p> <p>Observed the storage of devices to be decommissioned or reimaged to determine whether workstations to be decommissioned or reimaged are locked and maintained by the IT department.</p>	<p>No deviations noted.</p> <p>No deviations noted.</p>

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
	2. Disposal of assets are tracked by the IT Security Team to ensure assets are sanitized prior to disposal.	Inspected the log of all decommissioned assets to determine whether disposal of assets are tracked to ensure assets are sanitized prior to disposal.	No deviations noted.
6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
	1. Firewalls are in place to control and limit the type of network traffic allowed in and out of the network.	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.	No deviations noted.
	2. Antivirus software is installed on all DMI servers and workstations. The software scans machines for viruses in real-time.	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.	No deviations noted.
	3. 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.	Inspected the IDS/IPS console to determine whether the system is configured to send alerts to the IT Department when suspicious activity is detected.	No deviations noted.
		Inspected help desk tickets for a sample of IDS/IPS alerts to determine whether they are investigated and tracked to resolution.	No deviations noted.



Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
<b>6.7</b> The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
	1. All emails sent to external parties from the DMI domain are encrypted.	Inspected the email encryption settings to determine whether the system is configured to encrypt all outgoing emails from the DMI domain.	No deviations noted.
	2. Point-to-point encryption is utilized between DMI and BKFS MSP to ensure data transmission is secure.	Inspected the communications and mechanisms used for transmission of data between DMI and BKFS MSP to determine whether transmissions are encrypted.	No deviations noted.
	3. The web interface is secured with TLS encryption.	Observed a user access the web interface to determine whether TLS encryption is used.	No deviations noted.
	4. All laptop workstation hard drives are encrypted.	Inspected the Bitlocker management console for a sample of laptops to determine whether the hard drives are encrypted.	No deviations noted.
<b>6.8</b> The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
	1. 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.	Inspected the IDS/IPS console to determine whether the system is configured to send alerts to the IT Department when suspicious activity is detected.	No deviations noted.
		Inspected help desk tickets for a sample of IDS/IPS alerts to determine whether they are investigated and tracked to resolution.	No deviations noted.

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
	2. Inbound emails are automatically scanned for viruses and malware and suspicious emails are automatically quarantined.	Inspected the antivirus gateway settings to determine whether emails are set to be automatically scanned for viruses and malware and suspicious emails are automatically quarantined.	No deviations noted.
	3. Antivirus software is installed on all DMI servers and workstations. The software scans machines for viruses in real-time.	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.	No deviations noted.
	4. Vulnerability scans are performed monthly by the IT Team and helpdesk tickets are created to address any findings as deemed necessary..	Inspected vulnerability scan results and corresponding helpdesk tickets for a sample of months to determine whether they are performed on a monthly basis and helpdesk tickets are created to address any findings as deemed necessary.	No deviations noted.

#### 7.0 Common Criteria related to Systems Operations

**7.1** To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.

1. 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.	Inspected the IDS/IPS console to determine whether the system is configured to send alerts to the IT Department when suspicious activity is detected.	No deviations noted.
	Inspected help desk tickets for a sample of IDS/IPS alerts to determine whether they are investigated and tracked to resolution.	No deviations noted.

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
	2. Inbound emails are automatically scanned for viruses and malware and suspicious emails are automatically quarantined..	Inspected the antivirus gateway settings to determine whether emails are set to be automatically scanned for viruses and malware and suspicious emails are automatically quarantined..	No deviations noted.
	3. Vulnerability scans are performed monthly by the IT Team and helpdesk tickets are created to address any findings as deemed necessary..	Inspected vulnerability scan results and corresponding helpdesk tickets for a sample of months to determine whether they are performed on a monthly basis and helpdesk tickets are created to address any findings as deemed necessary.	No deviations noted.
<b>7.2</b> The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
	1. 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.	Inspected the IDS/IPS console to determine whether the system is configured to send alerts to the IT Department when suspicious activity is detected.	No deviations noted.
		Inspected help desk tickets for a sample of IDS/IPS alerts to determine whether they are investigated and tracked to resolution.	No deviations noted.

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
	2. Vulnerability scans are performed monthly by the IT Team and helpdesk tickets are created to address any findings as deemed necessary..	Inspected vulnerability scan results and corresponding helpdesk tickets for a sample of months to determine whether they are performed on a monthly basis and helpdesk tickets are created to address any findings as deemed necessary.	No deviations noted.
	3. Firewalls are in place to control and limit the type of network traffic allowed in and out of the network.	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.	No deviations noted.
	4. Temperature sensors are in place and configured to send alerts to IT personnel when the temperature rises above a certain threshold.	Inspected the temperature alert settings for Lake Zurich and North Aurora data centers to determine whether temperature is monitored.	No deviations noted.
<b>7.3</b> The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
	1. The Incident Response Plan outlines the procedures to report incidents and is made readily available to employees on the internal document management portal.	Inspected the Incident Response Plan to determine whether it communicates how employees should follow the IRP to report incidents.	No deviations noted.
		Inspected the internal document management portal to determine whether the Incident Response Plan is readily available to employees.	No deviations noted.

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
7.4	2. All potential events and incidents are reported to the Legal Department via an Incident Report Form and is investigated and tracked until resolution.	Inspected the Incident Report Forms for a sample of events and incidents to determine whether events and incidents are documented and tracked until resolution.	No deviations noted.
	3. 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.	Inspected the IT Steering Committee minutes for a sample of months to determine whether security, availability, and confidentiality events and incidents are discussed during monthly IT Steering Committee meetings.	No deviations noted.
	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.		
	1. All potential events and incidents are reported to the Legal Department via an Incident Report Form and is investigated and tracked until resolution.	Inspected the Incident Report Forms for a sample of events and incidents to determine whether events and incidents are documented and tracked until resolution.	No deviations noted.
	2. The Incident Response Team and Security Administrator investigates and tracks identified incidents until resolution and notifies affected internal and/or external users.	Inquired with the Legal Counsel and Internal Audit Supervisor to obtain an understanding of the process for investigating, tracking, and communicating identified incidents.	No deviations noted.
	There were no incidents during the period. Therefore, there was no circumstance that warranted the performance of the control.	Inspected the Legal Department's event tracking log and inquired with the Legal Department and the Internal Audit Supervisor to verify that there were no incidents within the reporting period.	Not applicable. There was no circumstance that warranted the performance of the control. Accordingly, no testing was performed by us.

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
	<p>3. 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.</p>	<p>Inspected the IT Steering Committee minutes for a sample of months to determine whether security, availability, and confidentiality events and incidents are discussed during monthly IT Steering Committee meetings.</p>	<p>No deviations noted.</p>
7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
	<p>1. The Incident Response Team and Security Administrator investigates and tracks identified incidents until resolution and notifies affected internal and/or external users.</p>	<p>Inquired with the Legal Counsel and Internal Audit Supervisor to obtain an understanding of the process for investigating, tracking, and communicating identified incidents.</p>	<p>No deviations noted.</p>
	<p>There were no incidents during the period. Therefore, there was no circumstance that warranted the performance of the control.</p>	<p>Inspected the Legal Department's event tracking log and inquired with the Legal Department and the Internal Audit Supervisor to verify that there were no incidents within the reporting period.</p>	<p>Not applicable. There was no circumstance that warranted the performance of the control. Accordingly, no testing was performed by us.</p>
	<p>2. 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.</p>	<p>Inspected the IT Steering Committee minutes for a sample of months to determine whether security, availability, and confidentiality events and incidents are discussed during monthly IT Steering Committee meetings.</p>	<p>No deviations noted.</p>

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
	3. Data backup tape restores are performed by the IT System Administrators quarterly	Inspected restoration logs for a sample of quarters to determine whether single file restorations are tested quarterly.	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.	Inspected the Business Continuity Plan to determine whether it exists and identifies the warm-site and secondary disaster recovery facility.	No deviations noted.
	5. The BCP Committee reviews and documents the BKFS MSP Disaster Recovery test results annually.	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.	No deviations noted.
	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.	Inspected the Operational Disaster Recovery Exercise to determine whether disaster recovery tests are performed annually.	No deviations noted.

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
<b>8.0 Common Criteria related to Change Management</b>			
<b>8.1</b>	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.		
	1. 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.	Inspected the SDLC policy to determine whether it is formally documented and reviewed annually by the IT team.	No deviations noted.
	2. All changes must be authorized by a Team Lead or Manager prior to development.	Inspected the change tickets for a sample of changes to determine whether changes are authorized by a Team Lead or Manager prior to development.	No deviations noted.
	3. All changes must be tested by development staff, project management, or client based on the request type.	Inspected the change tickets for a sample of changes to determine whether testing is performed.	No deviations noted.
	4. 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.	Inspected notifications sent for a sample of changes that affected internal or external users to determine changes are evaluated and communicated to internal and external parties.	No deviations noted.
	5. All changes must be approved by the Development Manager or Director of IT after testing, prior to migration into production.	Inspected the change tickets for a sample of changes to determine whether all changes are approved by the Development Manager or Director of IT after testing, prior to migration into production.	No deviations noted.



Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
	6. Any changes required as a result of the risk assessment are tracked by the IT Steering Committee for completion.	Inspected the Information Technology Steering Committee Meeting minutes to determine whether changes from the risk assessment are tracked for completion.	100% of the population was tested. No deviations noted.

#### 9.0 Common Criteria related to Risk Mitigation

##### 9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.

1.	An enterprise-wide risk assessment representing all areas of the organization and an Information Security and System Risk Assessment are conducted annually by the Information Security Officer Committee.	Inspected the most recent Enterprise-Wide Risk Assessment and the Information Security and System Risk Assessment to determine whether they are conducted annually by the Information Security Officer Committee.	No deviations noted.
2.	Quarterly Information Security Officer Committee meetings are held to evaluate risks related to security, availability, and confidentiality.	Inspected the Information Security Officer Committee meeting minutes for a sample of quarters to determine whether quarterly Information Security Officer Committee meetings are held to evaluate risks related to security, availability, and confidentiality.	No deviations noted.
3.	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.	Inspected the Business Continuity Plan to determine whether it exists and identifies the warm-site and secondary disaster recovery facility.	No deviations noted.

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
<b>9.2</b> The entity assesses and manages risks associated with vendors and business partners.			
	<p>1. DMI has a formal vendor management program that identifies critical vendors and their functions and cross-references the vendors to the appropriate DMI department.</p> <p>The CFO assesses vendors for criticality classification on an annual basis and documents the assessment in the Critical Vendor Listing with Rotational Review Breakout.</p>	Inspected the DMI Vendor Management Policy to determine whether a vendor management policy exists.	No deviations noted.
		Inspected the Critical Vendor Listing with Rotational Review Breakout to determine whether the assessment identifies key vendors and the services provided.	No deviations noted.
		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.	No deviations noted.
	2. Vendor Risk Review is performed to restrict third party access to confidential data to authorized third parties.	Inspected the Vendor Risk Review for a sample of vendors with access to confidential data to determine whether Vendor Risk Review is performed to restrict third party access to confidential data to authorized third parties.	No deviations noted.
	3. The Legal Department evaluates confidentiality commitments from third parties as part of the vendor review to ensure they align with DMI's confidentiality commitments.	Inspected vendor assessments for new third parties to determine whether confidentiality commitments are evaluated to ensure they align with DMI's commitments.	<p>No deviations noted.</p> <p>100% of the population was tested.</p>

Criteria	DMI's Control	Testing Performed by Service Auditor	Results of Test
	<p>4. DMI performs vendor assessments for all critical vendors on an annual basis. The Internal Audit reviews vendor SOC reports and evaluates vendor overall performance against the objectives specified in service level agreements.</p>	<p>Inspected vendor assessment packets for a sample of critical vendors to determine whether vendor performance is monitored annually by the Internal Audit Team.</p>	<p>No deviations noted.</p>

## B. Availability

Criteria	DMI's Control	Test Performed by Service Auditor	Results of Test
<b>1.0 Additional Criteria for Availability</b>			
<b>1.1</b> The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.			
	<b>1.</b> 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.	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.	No deviations noted.
	<b>2.</b> The PRTG Network Monitoring software also monitors uptime, bandwidth, and system capacity.	Inspected the PRTG Network Monitoring software to determine whether the software monitors uptime, bandwidth, and system capacity monitoring.	No deviations noted.
	<b>3.</b> The impact of any new clients on the capacity of the current system is evaluated during the monthly IT Steering Committee meetings and changes are made as necessary.	Inspected the IT Steering Committee minutes for a sample of months to determine whether capacity of the current system is monitored.	No deviations noted.

Criteria	DMI's Control	Test Performed by Service Auditor	Results of Test
1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.		
	1. The 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.	Inspected backup schedules to determine whether differential backups are configured to be performed daily and full backups performed weekly.	No deviations noted.
		Inspected the backup alert settings to determine whether alerts are sent to the IT Department when backup jobs are not completed successfully.	No deviations noted.
	2. DMI backup tapes are rotated offsite by the IT System Administrators to a records management company weekly.	Inspected the offsite records management pickup manifests for a sample of weeks to determine whether backup tapes are rotated offsite weekly.	No deviations noted.
	3. 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.	Inspected the Business Continuity Plan to determine whether it exists and identifies the warm-site and secondary disaster recovery facility.	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	Observed the Lake Zurich data center to determine whether it is located on the third floor to protect against flooding.	No deviations noted.

Criteria	DMI's Control	Test Performed by Service Auditor	Results of Test
	<p>has a raised floor and equipment is stored on equipment racks.</p> <p>Equipment is stored on equipment racks at the backup data center in North Aurora.</p>	Observed the Lake Zurich and North Aurora data centers to determine whether equipment is stored on equipment racks.	No deviations noted.
5.	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.	Observed the data centers at Lake Zurich and North Aurora to determine whether production systems are connected to the UPS units.	No deviations noted.
6.	UPS units are scheduled to perform self-tests every two weeks.	Inspected the UPS settings for Lake Zurich and North Aurora to determine whether UPS units are scheduled to perform self-tests every two weeks.	No deviations noted.
7.	The data centers in Lake Zurich and North Aurora are temperature controlled via dedicated HVAC systems.	Observed the data centers at Lake Zurich and North Aurora to determine whether dedicated HVAC systems are installed.	No deviations noted.
8.	Temperature sensors are in place and configured to send alerts to IT personnel when the temperature rises above a certain threshold.	Inspected the temperature alert settings for Lake Zurich and North Aurora data centers to determine whether temperature is monitored.	No deviations noted.
9.	Fire extinguishers are placed throughout the Lake Zurich, North Aurora, and Elgin office facilities according to local fire code.	Observed all facilities to determine whether fire extinguishers are present throughout the office facilities.	No deviations noted.

Criteria	DMI's Control	Test Performed by Service Auditor	Results of Test
	<p>The Lake Zurich and North Aurora data centers are equipped with smoke detectors and electrically rated fire extinguishers.</p> <p>All fire extinguishers are serviced on a regular basis.</p>	<p>Observed the data centers at Lake Zurich and North Aurora facilities to determine whether electrically rated fire extinguishers and smoke detectors are installed in the data center.</p> <p>Inspected documentation of the most recent fire extinguisher inspection for all facilities to determine whether fire extinguishers are serviced at least annually.</p>	<p>No deviations noted.</p> <p>No deviations noted.</p>
	<p><b>10.</b> 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.</p>	<p>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.</p>	<p>No deviations noted.</p>
	<p><b>11.</b> DMI performs vendor assessments for all critical vendors on an annual basis. The Internal Audit reviews vendor SOC reports and evaluates vendor overall performance against the objectives specified in service level agreements.</p>	<p>Inspected vendor assessment packets for a sample of critical vendors to determine whether vendor performance is monitored annually by the Internal Audit Team.</p>	<p>No deviations noted.</p>
<b>1.3</b> The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
	<p><b>1.</b> UPS units are scheduled to perform self-tests every two weeks.</p>	<p>Inspected the UPS settings for Lake Zurich and North Aurora to determine whether UPS units are scheduled to perform self-tests every two weeks.</p>	<p>No deviations noted.</p>

Criteria	DMI's Control	Test Performed by Service Auditor	Results of Test
	2. Data backup tape restores are performed by the IT System Administrators quarterly.	Inspected restoration logs for a sample of quarters to determine whether single file restorations are tested quarterly.	No deviations noted.
	3. The BCP Committee reviews and documents the BKFS MSP Disaster Recovery test results annually.	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.	No deviations noted.
	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.	Inspected the Operational Disaster Recovery Exercise to determine whether disaster recovery tests are performed annually and during the reporting period.	No deviations noted.



## C. Confidentiality

Criteria	DMI's Control	Test Performed by Service Auditor	Results of Test
<b>1.0 Additional Criteria for Confidentiality</b>			
<b>1.1</b> The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
	1. A Records Retention Management Procedure is formally documented and is reviewed annually by senior management.	Inspected the Records Retention Management Procedure to determine whether it is formally documented and reviewed by senior management annually and during the reporting period.	No deviations noted.
	2. Data is archived in a document management system.	Observed the document management system to determine whether data is archived.	No deviations noted.
	3. The 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.	Inspected backup schedules to determine whether differential backups are configured to be performed daily and full backups performed weekly.	No deviations noted.
		Inspected the backup alert settings to determine whether alerts are sent to the IT Department when backup jobs are not completed successfully.	No deviations noted.
	4. The Servicing Systems Support Team reviews MSP data deletion rulesets annually to ensure retention requirements are being met.	Inspected the most recent review of MSP data deletion rulesets to determine whether deletion rulesets are configured to meet retention requirements.	No deviations noted.

Criteria	DMI's Control	Test Performed by Service Auditor	Results of Test
<b>1.2</b> The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			
	<b>1.</b> Automated scripts are in place to wipe local workstation drives on a daily basis.	Inspected the scripts in place to wipe local workstations on a daily basis to determine whether data is restricted from being stored on local drives.	No deviations noted.
	<b>2.</b> Rulesets are in place within MSP to automatically delete data for inactive loans.	Inspected MSP data deletion rulesets to determine whether the system is configured to automatically delete data for inactive loans.	No deviations noted.
	<b>3.</b> The Servicing Systems Support Team reviews MSP data deletion rulesets annually to ensure retention requirements are being met.	Inspected the most recent review of MSP data deletion rulesets to determine whether deletion rulesets are configured to meet retention requirements.	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

plantemoran.com