Minnesota Management and Budget: Enterprise Performance Management Data Warehouse Integrity Controls

Information Technology Performance Audit

October 2024

Financial Audit Division

Office of the Legislative Auditor

State of Minnesota

Financial Audit Division

The division has authority to audit organizations and programs in the state's executive and judicial branches, metropolitan agencies, several "semi-state" organizations, state-funded higher education institutions, and state-funded programs operated by private organizations.

Each year, the division selects several of these organizations and programs to audit. The audits examine the policies and procedures—called internal controls—of the organizations to ensure they are safeguarding public resources and complying with laws that govern their financial and program operations. In addition, the division annually audits the State of Minnesota's financial statements and the financial statements of three state public pension systems. The primary objective of these financial audits is to assess whether the statements fairly present the organization's financial position according to Generally Accepted Accounting Principles.

The Office of the Legislative Auditor (OLA) also has a Program Evaluation Division. The Program Evaluation Division's mission is to determine the degree to which state agencies and programs are accomplishing their goals and objectives and utilizing resources efficiently.

OLA also conducts special reviews in response to allegations and other concerns brought to the attention of the Legislative Auditor. The Legislative Auditor conducts a preliminary assessment in response to each request for a special review and decides what additional action will be taken by OLA.

For more information about OLA and to access its reports, go to: www.auditor.leg.state.mn.us.

OLA | OFFICE OF THE LEGISLATIVE AUDITOR

Judy Randall, Legislative Auditor
State of Minnesota

October 2, 2024

Members
Legislative Audit Commission

Members
Legislative Commission on Cybersecurity

Erin Campbell, Commissioner
Minnesota Management and Budget

Tarek Tomes, Commissioner and Chief Information Officer
Minnesota Information Technology Services

This report presents the results of our information technology performance audit of the Enterprise Performance Management data warehouse integrity controls, operated by Minnesota Management and Budget (MMB) and Minnesota Information Technology Services (MNIT). The objective of this audit was to determine if MMB and MNIT had adequate internal controls to help ensure data in the warehouse mirrored data found in the Statewide Integrated Financial Tools (SWIFT) and the Statewide Employee Management System (SEMA4) business systems.

This audit was conducted by Mark Mathison, CISA, CISSP, CPA Inactive (IT Audit Director); and IT auditors Deb Frost, CISA; Dustin Juell, CompTIA Security+; and Peng Xiong.

We received the full cooperation of MMB and MNIT staff while performing this audit, and we thank them for their participation.

Sincerely,

Judy Randall
Legislative Auditor

Lori Leysen, CPA
Deputy Legislative Auditor

Room 140 Centennial Building, 658 Cedar Street, St. Paul, MN 55155-1603 • Phone: 651-296-4708 • Fax: 651-296-4712
E-mail: legislative.auditor@state.mn.us • Website: www.auditor.leg.state.mn.us • Minnesota Relay: 1-800-627-3529 or 711

OLA

Table of Contents

OLA

Introduction

Minnesota Management and Budget (MMB), in partnership with Minnesota Information Technology Services (MNIT), provides State of Minnesota agencies with a data warehouse to query and manage financial, human resources, and learning management information. State agencies use these data to monitor their operations, perform financial analysis, and compile data for internal and external reports. In addition, MMB utilizes data within the data warehouse to help prepare the state's Annual Comprehensive Financial Report.

This information technology performance audit focused on internal controls necessary to help ensure that data copied to the warehouse is identical to the same data found in the production business systems, such as the Statewide Integrated Financial Tools (SWIFT) and the Statewide Employee Management System (SEMA4).

Internal controls are the policies and procedures management establishes to govern how an organization conducts its work and fulfills its responsibilities. A well-managed organization has strong controls across all of its internal operations. If effectively designed and implemented, controls help ensure, for example, that inventory is secured, computer systems are protected, laws and rules are complied with, and authorized personnel properly document and process financial transactions.

Minnesota Law Mandates Internal Controls in State Agencies

State agencies must have internal controls that:

- Safeguard public funds and assets and minimize incidences of fraud, waste, and abuse.
- Ensure that agencies administer programs in compliance with applicable laws and rules.

The law also requires the commissioner of Management and Budget to review OLA audit reports and help agencies correct internal control problems noted in those reports.

— *Minnesota Statutes* 2023, 16A.057

OLA

Report Summary

Conclusion

Minnesota Management and Budget (MMB) and Minnesota Information Technology Services (MNIT) had adequate controls for their Enterprise Performance Management (EPM) data warehouse to help ensure that data in the warehouse mirrored data found in the Statewide Integrated Financial Tools (SWIFT) and the Statewide Employee Management System (SEMA4) business systems.

We found that the processes used by MMB and MNIT to load data into the warehouse included sufficient data validation and integrity controls. Furthermore, MMB and MNIT had sufficient change management controls to ensure that data maintenance performed on SWIFT and SEMA4 would be synchronized with its data warehouse. Finally, MMB and MNIT generally implemented appropriate security controls to prevent unauthorized changes to data stored within the warehouse.

Nevertheless, during our audit, we identified some information security control weaknesses. The list of findings below and the full report provide more information about these concerns.

Findings and Recommendations

Finding 1. MMB and MNIT have not completed current risk or security control assessments of the data warehouse. (p. 14)

Recommendation

MMB and MNIT should complete required risk and security control assessments of the data warehouse.

Finding 2. MMB and MNIT did not regularly review and validate that user access to the data warehouse administrative tools were appropriate for an employee's job duties, as required by MNIT security standards. (p. 16)

Recommendation

MMB and MNIT should regularly review and validate that permissions granted to user accounts remain necessary, as required by MNIT security standards.

Finding 3. MMB and MNIT did not scan for vulnerabilities or misconfigurations on critical computer devices that support the Statewide Integrated Financial Tools (SWIFT), the Statewide Employee Management System (SEMA4), or the data warehouse. (p. 17)

Recommendations

- MMB and MNIT should ensure all critical computer devices are scanned for security vulnerabilities.
- If critical computer devices cannot be scanned, MMB and MNIT should seek an approved exception from the security requirements.

OLA

Background

Minnesota Management and Budget Overview

Minnesota Management and Budget (MMB) is responsible for managing state finances, payroll, and human resources.[1] To help fulfill the department's responsibilities, MMB provides computerized systems and services that support state operations in the areas of budgeting, accounting, payroll, human capital management, and reporting.[2] The department's services include support and maintenance—in partnership with Minnesota Information Technology Services (MNIT)—of the Statewide Integrated Financial Tools (SWIFT), the Statewide Employee Management System (SEMA4), and the Enterprise Performance Management (EPM) data warehouse.[3]

Statewide Integrated Financial Tools (SWIFT)

SWIFT is the state's online financial, accounting, procurement, and reporting system.[4] State agencies use SWIFT, or interface other governmental systems with SWIFT, for the following key business functions:

Accounting

- Accounts Payable
- Accounts Receivable
- Asset Management
- Billing
- Budgeting
- General Ledger
- Grants
- Project Costing
- Supplier Administration

Procurement

- Contracts
- General Procurement
- Purchasing
- Purchasing Cards
- Receipts
- Requisitions
- Strategic Sourcing[5]

[1] MMB's roles and responsibilities are defined in *Minnesota Statutes* 2023, Chapters 16A and 43A.

[2] *Minnesota Statutes* 2023, 16A.15, subd. 2, mandates that MMB have an accounting system.

[3] Under *Minnesota Statutes* 2023, 16E.01, subd. 1a, MNIT is the state's centralized information technology department tasked with providing oversight, leadership, and direction for information and telecommunications technology policy. MNIT is also tasked with the management, delivery, accessibility, and security of executive branch information and telecommunications technology systems and services.

[4] SWIFT is a customized off-the-shelf (Oracle's PeopleSoft Financials and Supply Chain Management) software application designed to manage various financial, accounting, and procurement business processes.

[5] The Strategic Sourcing module in SWIFT provides a mechanism to solicit bids for the purchase of goods or services.

Statewide Employee Management System (SEMA4)

SEMA4 is the state's online human resources, payroll, benefits, and reporting system; the "4" in SEMA4 refers to these four main features, utilized by state agencies to:[6]

- Process and approve payroll.
- Recruit and manage employee information.
- Register, approve, deliver, and track educational courses and content provided to employees.
- Review current employee benefits and make allowable changes.
- Track and maintain job positions.

Current—and many former state employees—can access the system's "self-service" environment online to perform a variety of activities, including to:

- Approve timesheets submitted by subordinates.
- Change benefit and demographic data.
- Enter hours worked and leave taken.
- View payroll notices, leave balances, and W-2 forms.

Enterprise Performance Management (EPM) Data Warehouse

Although SWIFT and SEMA4 have built-in reporting capabilities, MMB developed and maintains—in partnership with MNIT—a data warehouse to assist agencies with ad hoc financial, human resources, and learning management reporting.[7] MMB's data warehouse also supports public disclosure of information, whereby citizens can utilize a web portal to explore state budgets and payment information.[8]

[6] SEMA4 is a customized off-the-shelf (Oracle's PeopleSoft Human Capital Management) software application designed to manage various human resources processes.

[7] MMB and MNIT utilize Oracle's Enterprise Performance Management platform as the base application for the data warehouse.

[8] *Minnesota Statutes* 2023, 16A.056, requires MMB to provide the public with a searchable database with information on state appropriations, contracts, and expenditures. Accordingly, MMB and MNIT maintain the following website: https://mn.gov/mmb/transparency-mn/.

A data warehouse can be defined as a central repository of information specifically designed for analysis and that can be used to improve decision-making. Data move into a data warehouse from transactional systems, relational databases, and other sources on a regular schedule. Users can pull data to perform analysis by using business intelligence tools, structured query language (SQL) clients, and other analytics applications. These tools allow state employees access to read-only data to query, analyze, and manage financial, human resources, and learning management data.

MMB organizes its data warehouse by subject areas. Current subject areas include:

- Financial Management Solutions (FMS)
  - Accounts Payable
  - Accounts Receivable
  - Expenditures and Receipts
  - General Ledger
  - Projects and Grants
- Supply Chain Management (SCM)
  - Encumbrances
  - Procurements
- Human Capital Management (HCM)
  - Payroll
  - Workforce and Learning
  - Recruiting Solutions

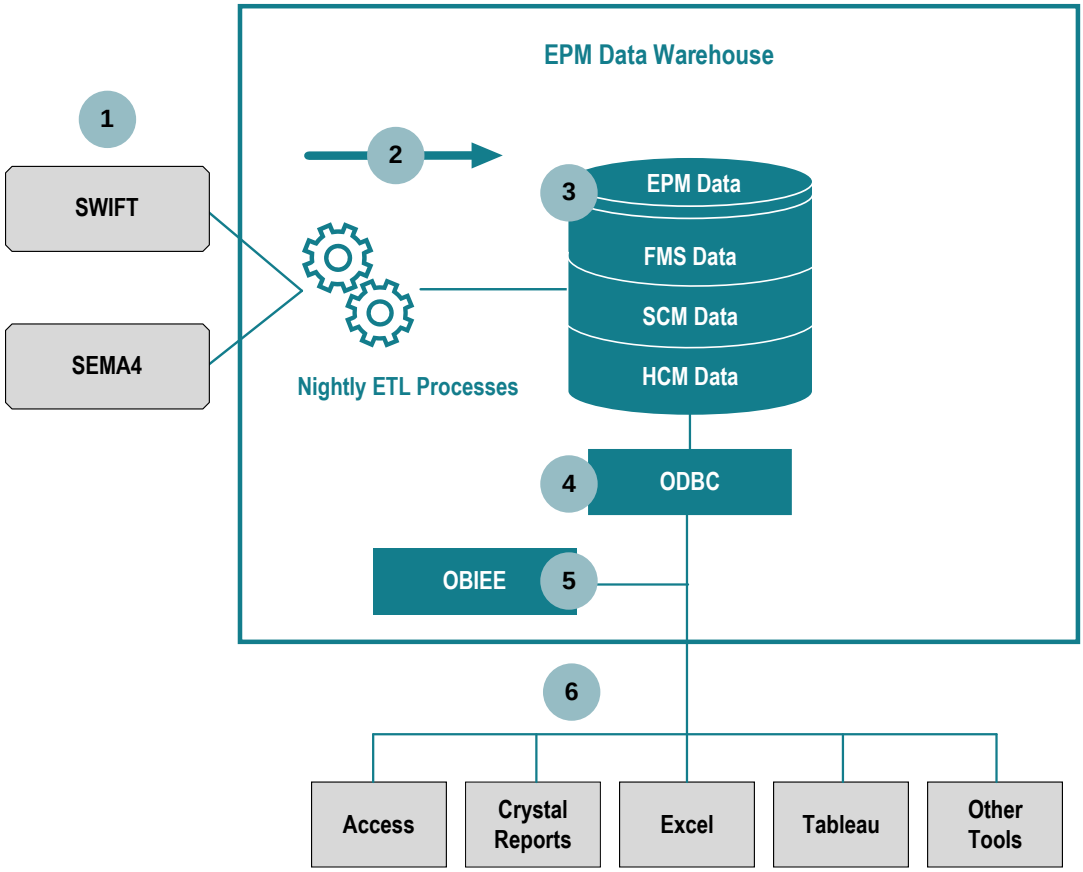
EPM Data Warehouse

As of December 2023, the EPM data warehouse extracted data from more than 650 SWIFT and SEMA4 production database tables, resulting in nearly 4.5 billion rows of financial, human resources, and learning management data.

While many state employees access the data using a web-based Oracle Business Intelligence Enterprise Edition (OBIEE) tool, other third-party tools can be used to extract and report the data. Exhibit 1 provides a high-level overview of six key components of the data warehouse environment.

Exhibit 1

Overview of the Data Warehouse Environment



Notes: Data warehouse components include items 2 through 5. Items 1 and 6 are other technologies outside the boundaries of the data warehouse. The numbered components in the diagram are as follows:

1. Source business systems, including SWIFT and SEMA4.
2. Nightly processes extract, transform, and load (ETL) data from the source systems into the data warehouse. ETL uses a set of business rules to clean and organize raw data and prepare it for storage, data analytics, and machine learning.
3. Enterprise Performance Management (EPM) data separated by subject areas: Financial Management Solutions (FMS), Supply Chain Management (SCM), and Human Capital Management (HCM).
4. Open Database Connectivity (ODBC) allows an interface for user reporting.
5. Oracle Business Intelligence Enterprise Edition (OBIEE) allows for more efficient analysis of the data.
6. Third-party reporting tools provide advanced users with optional reporting and data extraction methods.

Source: Office of the Legislative Auditor.

With state agencies relying on the nearly 4.5 billion rows of financial and human resources data within MMB's data warehouse, it is essential to have internal controls that help ensure both the accuracy and completeness of the data.[9] Further, strong security controls help protect data from unauthorized changes or errors in processing.

In some cases, information system professionals must correct data errors in SWIFT and SEMA4 production business systems. When such corrections are necessary, MMB and MNIT need controls to synchronize data maintenance between their business systems and their data warehouse. Without synchronization, data fixes in SWIFT and SEMA4 could lead to a gradual degradation of warehouse data integrity.

Audit Scope, Objectives, Methodology, and Criteria

We conducted this information technology performance audit to determine whether MMB and MNIT followed applicable policies, standards, and best practices designed to protect the integrity of the statewide EPM data warehouse. We evaluated policies, procedures, and controls during the period from November 2023 through March 2024.

We designed our work to address the following questions:

- Did MMB and MNIT have internal controls to ensure that data loaded into the data warehouse were accurate and complete?
- Did MMB and MNIT have procedures to synchronize data maintenance between the SWIFT and SEMA4 production business systems and the data warehouse?
- Did MMB and MNIT have appropriate security administration procedures to prevent unauthorized or erroneous changes to the data warehouse?

To answer these questions, we:

- Reviewed MMB's and MNIT's documentation.
- Interviewed staff at MMB and MNIT.
- Performed data analysis to reconcile SWIFT source system data to data in the warehouse.
- Evaluated change management processes at MMB and MNIT.
- Reviewed and validated current data warehouse system configuration documentation, security assessments, and vulnerability scans.
- Examined user account access privileges and security policies.

[9] Data integrity controls help ensure that data copied to the warehouse are identical to the same data found in the production business systems, such as SWIFT and SEMA4.

Using applicable federal and state laws, and agency policies and standards, we tested whether MMB and MNIT had effective information security controls in place to protect the integrity of the data warehouse.

We conducted this performance audit in accordance with generally accepted government auditing standards.[10] Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

To assist with our testing and data validation, we obtained access to SWIFT, SEMA4, and the EPM data warehouse. When sampling was used, we used a sampling method that complies with generally accepted government auditing standards and that supports our findings and conclusions. That method does not, however, allow us to project the results we obtained to the populations from which the samples were selected.

[10] Comptroller General of the United States, Government Accountability Office, *Government Auditing Standards, 2018 Revision* (Washington, DC, Technical Update April 2021).

Warehouse Data Integrity Controls

Extract, Transform, and Load

Minnesota Management and Budget (MMB) and Minnesota Information Technology Services (MNIT) use various extract, transform, and load (ETL) processes to copy relevant data from Statewide Integrated Financial Tools (SWIFT) and the Statewide Employee Management System (SEMA4) into its data warehouse. ETL uses a set of business rules to clean and organize the data and prepare it for storage, data analytics, and machine learning.

ETL works by moving data from the source system to the destination system at periodic intervals. The ETL process works in three steps:

1. Extract the relevant data from the source database
2. Transform the data so that it is better suited for analytics
3. Load the data into the target database

MMB's and MNIT's ETL process consists of two load types. The first, Operational Warehouse Staging (OWS), serves as a "receiving area" for data extracted from SWIFT and SEMA4. The second uses additional ETL processes to move data into the multidimensional warehouse—a technology solution that enables more efficient analysis of the data.

Most agency end users use business intelligence reporting tools, such as Oracle Business Intelligence Enterprise Edition (OBIEE), to analyze SWIFT and SEMA4 data that have been loaded into the multidimensional warehouse. Some agency staff use other third-party reporting tools to access the data, connecting directly to staging tables and views in OWS.

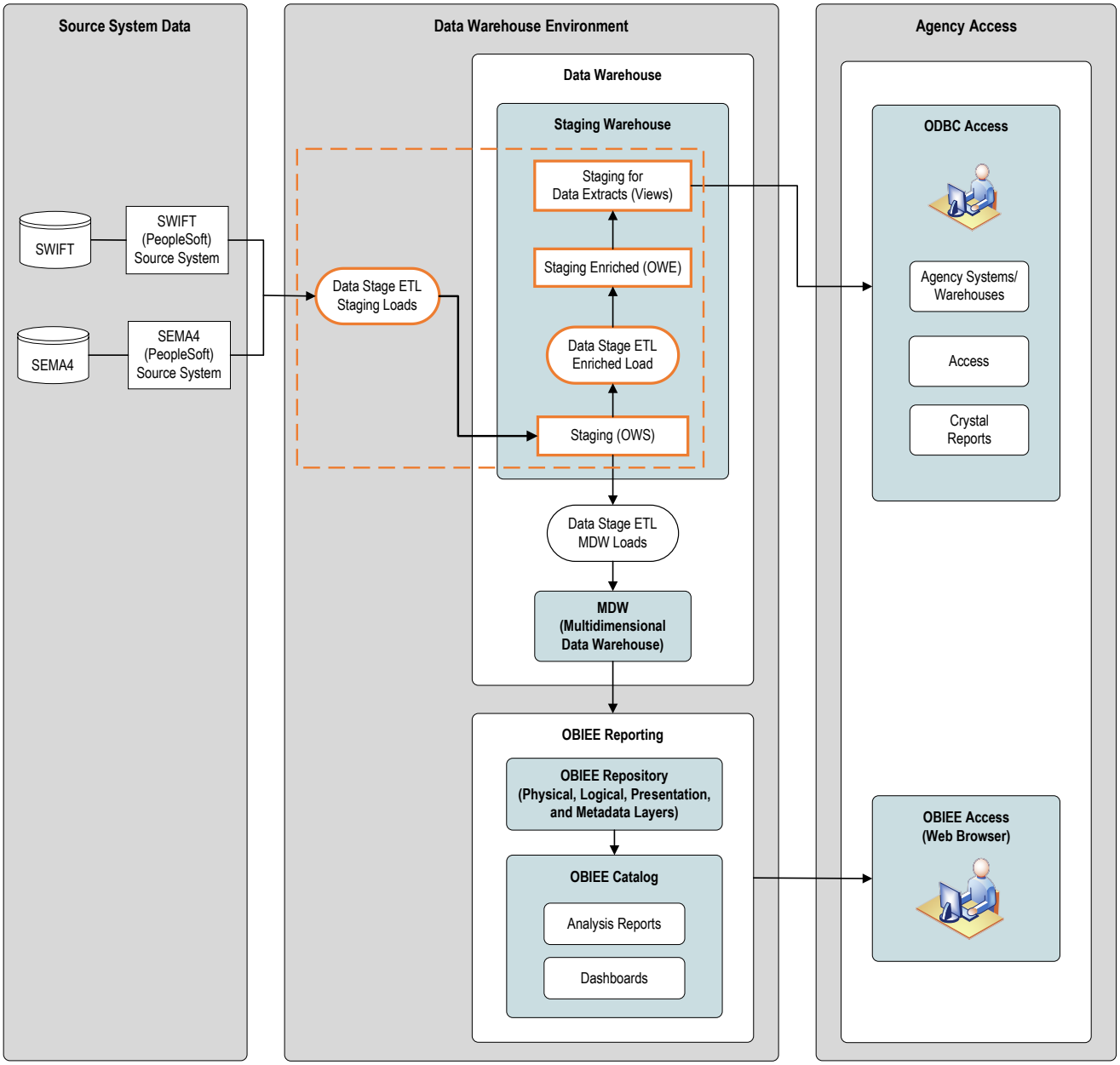
The scope of our audit focused on the OWS environment, as these components of the architecture serve as the basis for data analysis within the EPM data warehouse. MMB also uses data directly from OWS to produce the state's Annual Comprehensive Financial Report. Exhibit 2 helps articulate the scope of our work.

To gain an understanding of MMB's and MNIT's relevant internal controls, we interviewed staff responsible for developing, maintaining, and monitoring computer programs and tools used to extract, transform, and load data. We observed certain error-handling processes to validate that data integrity controls were appropriately designed and implemented. Finally, we tested 167 sample transactions to confirm that approximately 2,800 data elements loaded accurately into OWS.

We concluded that MMB and MNIT had adequate internal controls to ensure that the data transferred to the warehouse were both accurate and complete. During our audit, we found no significant issues.

Exhibit 2

MMB Enterprise Performance Management Data Warehouse – Scope of Audit



Note: We included in our audit scope the areas outlined in the dashed orange box.

Source: Office of the Legislative Auditor.

Change Management Controls

This part of the audit focused on internal controls designed to help manage changes to the computers, software programs, and data relevant to the data warehouse. In some cases, information system professionals must correct data errors in SWIFT and SEMA4 production business systems. When this occurs, MMB and MNIT need controls to synchronize data maintenance between their business systems and their data warehouse. Without synchronization, data fixes in SWIFT and SEMA4 could lead to a gradual degradation of warehouse data integrity.

To conduct our work, we interviewed staff and reviewed relevant documents to understand the processes for requesting, approving, and implementing changes. We validated whether controls were implemented by identifying recent changes and reviewing supporting evidence. We reviewed relevant communications to determine if stakeholders were informed and involved in change processes. Additionally, as part of our extract, transform, and load testing, we determined if MMB and MNIT were utilizing vendor-recommended data validation controls to help identify and load any changed source data. Finally, to confirm separation of duties of those staff involved, we reviewed access permissions for requesting, approving, and implementing changes to the data warehouse.

We concluded that MMB and MNIT had adequate internal controls to manage changes to their environment and to synchronize data maintenance between their business systems and their data warehouse. During our audit, we found no significant issues.

Data Integrity Security Controls

This part of the audit focused on security controls designed to help protect data from unauthorized changes. We gained an understanding of the controls in place and, based on our assessment of risk, tested significant controls within the data warehouse against key MNIT technical security policies and standards.[11] Our audit looked at the following information security areas:

- Identity and access management
- Information security risk management
- Secure system configuration
- Security logging and monitoring
- Threat and vulnerability management

We concluded that MMB and MNIT had generally implemented appropriate security controls to prevent unauthorized changes to warehouse data. However, we identified

[11] Minnesota Information Technology Services, *Enterprise Information Security Policies and Standards*, https://mn.gov/mnit/government/policies/security/, accessed July 12, 2024.

some weaknesses that the departments should address to improve their control structure of the warehouse. We discuss these weaknesses in more detail below.

Information Security Risk Management

MMB's risk assessment procedure and MNIT's information security standard require applicable state agencies to perform risk assessments.[12] MMB's procedure requires agencies to annually conduct a comprehensive review of their most significant business processes and risks. MNIT requires information security risk and security control assessments be completed on all new and significantly changed systems. For systems like SWIFT, SEMA4, and the data warehouse, risk assessments must be updated at least every three years, while security control assessments must be performed annually.[13] The information security risk management standard further requires that agencies document the results of the assessments in reports that can be shared with agency leadership and other stakeholders. MNIT's process for managing security risks is outlined in the Appendix. Although MMB had completed a risk assessment of its business processes, MMB and MNIT did not complete risk or security control assessments of the data warehouse.

FINDING 1

MMB and MNIT have not completed current risk or security control assessments of the data warehouse.

MNIT developed a risk and security control document template that it provides to agencies to complete for each system of a specific risk level. MNIT designed the template to help agencies evaluate risks to their system(s) and self-assess compliance with approximately 250 security controls. If control gaps in the data warehouse are identified—whether by agency staff, information security professionals, or internal or external auditors—it begins the process for MMB management to either accept the risks resulting from the deficiency, or develop remediation plans to mitigate the control gaps identified. Despite the data warehouse being in operation since 2012, and recently undergoing significant changes, MMB and MNIT have never completed a risk assessment or a security control assessment.

Having an accurate assessment of controls is essential for risk management processes. Agency representatives recognized the importance of the risk and security control assessments, and told us that they have had numerous internal discussions regarding risks associated with the data warehouse. However, they told us that system changes and resource constraints caused them to prioritize other work and not complete the risk and security control assessments as required by MNIT's risk-management standard. When risk management processes are not completed, agency leaders may not have a complete and accurate picture of their agency's information technology

[12] Minnesota Management and Budget, Statewide Operating Procedure 0102-01.2, *Risk Assessment*, April 10, 2023; and Minnesota Information Technology Services, *Information Security Risk Management Standard*, version 1.7, October 1, 2023.

[13] Minnesota Information Technology Services, *Information Security Risk Management Standard*, version 1.7, Controls 2 and 3, October 1, 2023.

risks. Without fully understanding their risk posture, leaders may fail to address critical cybersecurity weaknesses.

RECOMMENDATION

MMB and MNIT should complete required risk and security control assessments of the data warehouse.

Identity and Access Management

Identity and access management consists of three key activities: (1) identifying individual data warehouse users, (2) defining how those users access the data warehouse, and (3) establishing what functions they can access within the data warehouse. The data warehouse has primarily two user types that can log into and access the system:

1. **Administrative users.** These accounts have the ability to upload and update data and maintain the data warehouse.[14]

2. **End users.** These accounts have read-only access to query the data and develop financial, human resources, and learning management reports, charts, and dashboards.

Identity and access management extends beyond the data warehouse itself. It also includes defining and controlling necessary access to servers, databases, and various other system components and supporting tools that interact with the data warehouse. MNIT defines expected controls within its identity and access management policy and standard.[15] The security standard outlines more than 40 related controls; we evaluated compliance with these controls based on risk to the data warehouse.

Our testing focused on 26 of the key controls related to user accounts and authentication for the data warehouse and its underlying components. These control requirements help protect MMB and MNIT from inappropriate persons accessing the data warehouse, and limit access to only information that is necessary to perform job duties. In general, we found that MMB and MNIT complied with required identity and access management controls. However, we found a weakness with 1 of the 26 controls tested.

MNIT's security standards require that a process must exist to regularly review, validate, and recertify that access to the data warehouse is still appropriate.[16] Although MMB's

[14] For our audit, we categorized service accounts as administrative users. A service account is a special kind of account typically used by an application or computer batch process, rather than a person.

[15] Minnesota Information Technology Services, *Identity and Access Management Policy*, version 1.5, October 1, 2022; and Minnesota Information Technology Services, *Identity and Access Management Standard*, version 1.6, October 1, 2022. In January 2024, MNIT released version 1.7 of its standard, which added three new controls that we did not include in the scope of this audit.

[16] MNIT security standards require supervisors and managers to review all general user accounts at least annually and all privileged accounts at least semiannually. (Minnesota Information Technology Services, *Identity and Access Management Standard*, version 1.6, Control 6, October 1, 2022; and Minnesota Information Technology Services, *Privileged Account Management Standard*, version 1.0, February 1, 2023.)

security procedures require an annual statewide review of access to SWIFT and SEMA4, including end-user access to the data warehouse, no process existed to regularly review access to the warehouse's administrative tools.[17]

FINDING 2

MMB and MNIT did not regularly review and validate that user access to the data warehouse administrative tools were appropriate for an employee's job duties, as required by MNIT security standards.

MMB annually sends instructions to state agencies to recertify access for their respective staff. MMB itself had completed its own annual recertifications of staff with access to human resources, payroll, accounting, and warehouse data. However, the access reviews it had conducted were limited to accounts within the business applications and did not include a review of the administrative accounts with access to the computers, databases, programs, and administrative tools that support the data warehouse.[18] A MNIT representative indicated that MMB and MNIT did not consider reviewing access to the administrative tools as part of MMB's standard application access reviews.

The lack of recertifications increases the risk of inappropriate or unneeded access to the data warehouse. MMB and MNIT have many staff with access to financial and human resources systems and data; as a result, validation of security permissions is critical. During our audit, we found some examples of MNIT staff supporting the data warehouse who had security permissions and roles that may not have aligned with their job duties. For example, we found some instances where system programmers and database administrators had administrative permissions to change management tools. In general, system programmers should not have the ability to move computer code into the operational environment and should not have access to operational software or data. Similarly, database administrators should not be involved in IT management functions beyond the duties of database administration. If MMB and MNIT had conducted the reviews as required, they would have identified staff who had unneeded access to certain administrative functions within the data warehouse.

RECOMMENDATION

MMB and MNIT should regularly review and validate that permissions granted to user accounts remain necessary, as required by MNIT security standards.

[17] Minnesota Management and Budget, Statewide Operating Procedure 1101-07.1, *Agency Security Administrators*, Steps 9 and 10, July 1, 2011.

[18] In addition to accounts within SWIFT, SEMA4, and the EPM data warehouse, MMB—as owner of the system—needs to review accounts within administrative tools, change management software, databases, and the computers that support the system. Because MNIT provides operational support of these systems, the reviews need to be completed in partnership with MNIT management.

Threat and Vulnerability Management

Threat and vulnerability management is a risk-based approach to discovering, prioritizing, and remediating vulnerabilities and misconfigurations in IT environments. MNIT's threat and vulnerability management standard sets the baseline requirements for executive branch agencies to identify, prioritize, and address information security threats and vulnerabilities.[19]

MNIT has developed a centralized process to scan all agency computers in MNIT's physical and cloud data centers for both vulnerabilities and compliance with baseline configuration standards. To be effective, MNIT requires state entities to install software—called an "agent"—on each device that needs to be tested.[20] Once installed, the agent gathers information that shows whether the device has vulnerability or configuration problems and reports the results to a central console, which is reviewed by MNIT staff.

We tested 35 sample computer devices that support the statewide EPM data warehouse to validate that security scanning occurred and that identified vulnerabilities or misconfigurations were included in a remediation plan.[21] In general, MMB and MNIT were scanning, detecting, and resolving system-identified issues. However, during our testing, we found that MMB and MNIT did not scan some critical servers for security vulnerabilities.

FINDING 3

MMB and MNIT did not scan for vulnerabilities or misconfigurations on critical computer devices that support the Statewide Integrated Financial Tools (SWIFT), the Statewide Employee Management System (SEMA4), or the data warehouse.

When we reviewed MNIT's scanning processes, we discovered that MMB and MNIT had not installed necessary scanning agents onto critical computers that support the system. In response to our questions, MMB and MNIT told us that the support agreement with an outside vendor, who maintains the hardware and software, prohibits installation of the scanning agents. MMB and MNIT noted that, because the vendor has other system security controls in place, they believed this to be lower risk. However, MMB and MNIT had not followed risk-acceptance processes to seek an approved

[19] Minnesota Information Technology Services, *Threat and Vulnerability Management Standard*, version 1.7, October 1, 2023.

[20] Minnesota Information Technology Services, *Secure Configuration Standard*, version 1.7, Control 34, October 1, 2023.

[21] A computer device may include servers, workstations, networking components, or other technologies that are connected to the data warehouse network.

exception from their leadership to the vulnerability scanning requirements.[22] MNIT staff specializing in vulnerability scanning further noted that, while the installation of software agents is the preferred method to achieve results, MNIT can scan for vulnerabilities using other methods that do not rely upon the scanning agents. MMB and MNIT were not using any alternative methods for scanning critical servers for security vulnerabilities.

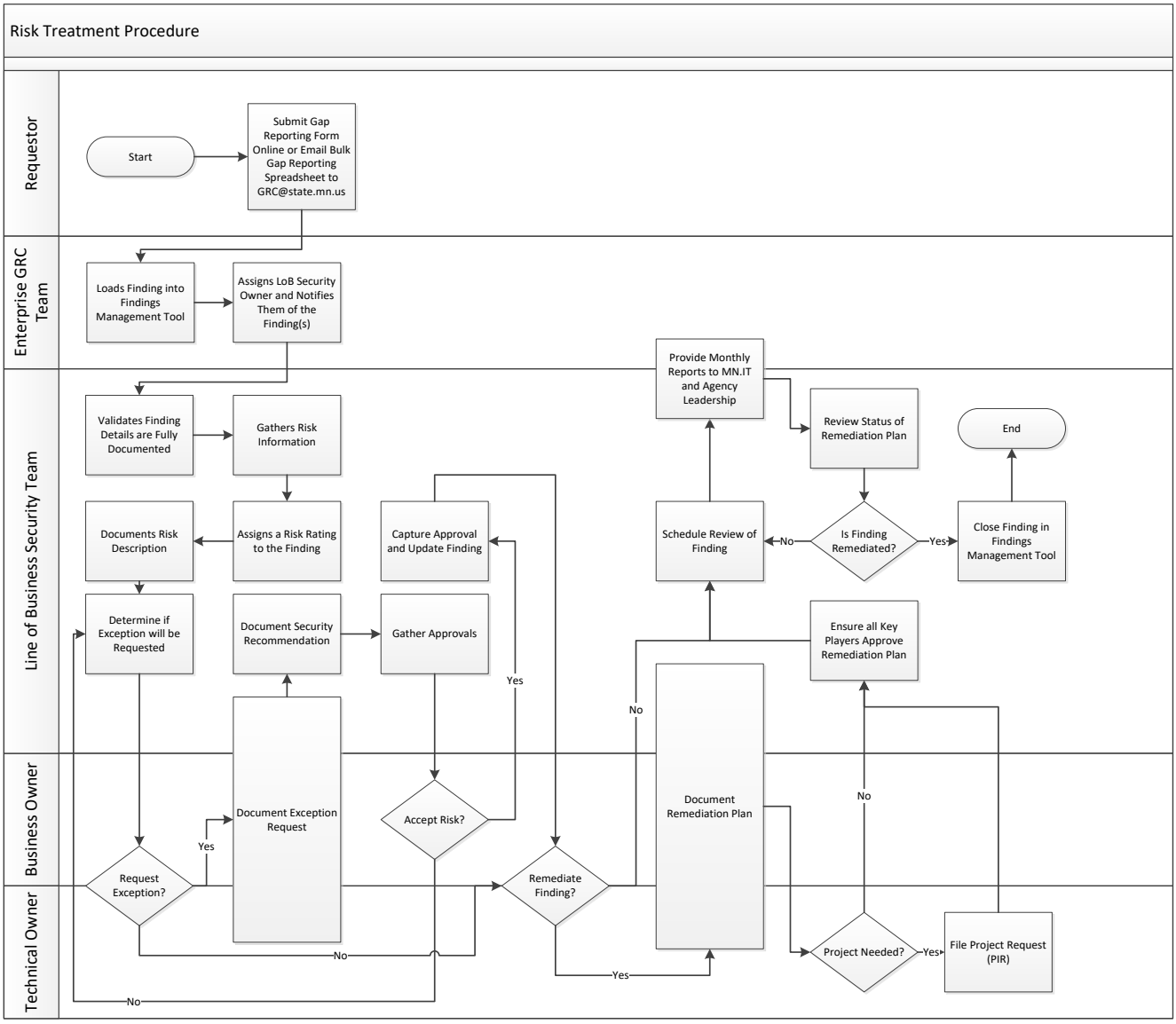
By not scanning for vulnerabilities, MMB and MNIT may not be identifying—and resolving—all possible vulnerabilities on some of the system's most critical devices.

RECOMMENDATIONS

- **MMB and MNIT should ensure all critical computer devices are scanned for security vulnerabilities.**
- **If critical computer devices cannot be scanned, MMB and MNIT should seek an approved exception from the security requirements.**

[22] Minnesota Information Technology Services, *Information Security Program Standard*, version 1.7, Control 4, October 1, 2023, stipulates that the state's Chief Information Security Officer or delegate must approve any exceptions to the policies and standards. Minnesota Information Technology Services, *Information Security Risk Treatment Procedure*, version 1.0, January 1, 2017, outlines the steps for requesting and approving an exception.

Appendix: MNIT's Information Security Risk Treatment Procedure



Source: Minnesota Information Technology Services, *Information Security Risk Treatment Procedure*, version 1.0, January 1, 2017.

OLA

MINNESOTA

September 25, 2024

Judy Randall, Legislative Auditor
Office of the Legislative Auditor
140 Centennial Office Building
658 Cedar Street Saint Paul, MN 55155

Dear Auditor Randall:

Thank you for the opportunity to respond to the audit report reviewing the Enterprise Performance Management (EPM) Data Warehouse integrity controls. Minnesota IT Services (MNIT) and Minnesota Management and Budget (MMB) value the important role the Office of the Legislative Auditor (OLA) serves to improve government accountability and enhance program effectiveness.

Audit reports aid our agencies in ensuring that we are operating our programs and services at the highest levels possible, and we welcome the feedback provided by the audit team. We are pleased that the report concluded that MMB and MNIT generally had adequate and sufficient controls and processes for data validation and integrity, change management, and unauthorized change security related to the EPM Data Warehouse. Below you will find a combined detailed response to the OLA's audit findings and recommendations for MNIT and MMB. Overall, we appreciate the opportunity to improve the operational effectiveness and risk mitigation activities related to systems within the data warehouse. As noted below, MNIT and MMB have fully resolved two of the three findings, and anticipate resolution of the third finding shortly after the public release of this report.

Response to the OLA's Findings and Recommendations

OLA Finding 1

- *MMB and MNIT have not completed current risk or security control assessments of the state's data warehouse.*

OLA Recommendations pertaining to Finding 1

- MMB and MNIT should complete required risk and security control assessments of the state's data warehouse.

We agree with the OLA's finding and support the OLA's recommendations. MNIT and MMB acknowledge that there is not a current risk or security control assessment on file and is in the process of completing the required risk and security control assessments for the EPM Data Warehouse. MNIT and MMB anticipate this assessment will be completed shortly after the public release of the audit report. We would also note that while formal risk and security assessments using MNIT's template have not been completed, the agencies have evaluated and identified risks and testified to those risks when pursuing critical funding to address operational and security gaps. Recognizing these needs, the legislature provided critical investments and funding adjustments in the 2023 legislative session.

OLA Finding 2

- *MMB and MNIT did not regularly review and validate that user access to the data warehouse administrative tools were appropriate for an employee's job duties, as required by MNIT security standards.*

OLA Recommendations pertaining to Finding 2

- MMB and MNIT should regularly review and validate that permissions granted to user accounts remain necessary, as required by MNIT security standards.

We agree with the OLA's finding and support the OLA's recommendations. MNIT and MMB acknowledge that at the time of the audit, there had not been a formal review of permissions granted to user accounts for the MNIT teams that provide direct IT support to the EPM Data Warehouse and supporting administrative tools. Upon notification of this gap, MNIT and MMB immediately began to address this review, which is now complete. MNIT and MMB have further developed internal processes for reviews to be completed on an annual basis. This finding has been resolved.

OLA Finding 3

- *MMB and MNIT did not scan for vulnerabilities or misconfigurations on critical computer devices that support the Statewide Integrated Financial Tools (SWIFT), the Statewide Employee Management System (SEMA4), or the statewide data warehouse.*

OLA Recommendations pertaining to Finding 3

- MMB and MNIT should ensure all critical computer devices are scanned for security vulnerabilities.
- If critical computer devices cannot be scanned, MMB and MNIT should seek an approved exception from the security requirements.

We agree with the OLA's finding and support the OLA's recommendations. We are pleased to report that our MNIT team has now implemented scanning for security and misconfiguration vulnerabilities on these devices. This finding has been resolved.

Additional context on security and misconfiguration vulnerability scanning

The computer devices relevant to this finding, while previously lacking comprehensive scanning tools, were not lacking in all security controls. These specific devices are highly controlled vendor-supplied hardware and software, which utilize vendor-provided security controls to ensure optimal performance per vendor specifications. In addition, MNIT utilizes additional security controls to mitigate risk related to these systems. While scanning is a necessary component of risk mitigation, it is important to articulate that vulnerability risks on these critical devices were actively being managed.

Once again, thank you for the opportunity to respond to the OLA's report.

Sincerely,

Tarek Tomes
Commissioner, MNIT Services

Erin Campbell
Commissioner, Minnesota Management and Budget

OLA

OLA

Financial Audit Staff

Judy Randall, *Legislative Auditor*
Lori Leysen, CPA, *Deputy Legislative Auditor*

Audit Directors
Ryan Baker, CFE
Jordan Bjonfald, CPA
Kayla Borneman, CPA
Mark Mathison, CISA, CISSP, CPA (inactive)
Heather Rodriguez
Valentina Stone, CPA
Scott Tjomsland, CPA
Zach Yzermans, CPA

Audit Coordinators
Joe Sass, CISA

Audit Team Leads
Shannon Hatch, CFE
Gabrielle Johnson, CPA
Holly Runia

Senior Auditors
Tyler Billig, CPA
Deb Frost, CISA
Lisa Makinen, CPA
Alec Mickelson
Duy (Eric) Nguyen
Crystal Nibbe, CFE
Erick Olsen
Zakeeyah Taddese
Emily Wiant

Auditors
Joseph Anderson
Ria Bawek
Nicholai Broekemeier
Gabrielle Gruber
Dylan Harris
Nicole Heggem
Andrea Hess
Dustin Juell, CompTIA Security+
Christian Knox
Sheena Kurth
Benjamin Path
Peng Xiong

For more information about OLA and to access its reports, go to: www.auditor.leg.state.mn.us.

To offer comments about our work or suggest an audit, evaluation, or special review, call 651-296-4708 or e-mail legislative.auditor@state.mn.us.

To obtain printed copies of our reports or to obtain reports in electronic ASCII text, Braille, large print, or audio, call 651-296-4708. People with hearing or speech disabilities may call through Minnesota Relay by dialing 711 or 1-800-627-3529.

 Printed on Recycled Paper

OLA | OFFICE OF THE LEGISLATIVE AUDITOR

Office of the Legislative Auditor
Suite 140
658 Cedar Street
Saint Paul, MN 55155