OLA
OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

FINANCIAL AUDIT DIVISION REPORT

Office of MN.IT Services

Mainframe Security Controls

May 1, 2014 **Report 14-14**

FINANCIAL AUDIT DIVISION
Centennial Building – Suite 140
658 Cedar Street – Saint Paul, MN 55155
Telephone: 651-296-4708 • Fax: 651-296-4712
E-mail: legislative.auditor@state.mn.us
Web site: http://www.auditor.leg.state.mn.us
Through Minnesota Relay: 1-800-627-3529 or 7-1-1

OFFICE OF THE LEGISLATIVE AUDITOR
State of Minnesota • James Nobles, Legislative Auditor

May 1, 2014

Senator Roger Reinert, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Carolyn Parnell, Commissioner
Office of MN.IT Services

This report presents the results of our audit of the internal controls over the Office of MN.IT Services' mainframe security as of October 2013.

We discussed the results of the audit with the Office of MN.IT Services' staff on April 10, 2014. This audit was conducted by Carolyn Engstrom, CPA, CISA (Audit Manager) and David Westlund, CPA, CISA (Auditor-in-Charge).

We received the full cooperation of the Office of MN.IT Services' staff while performing this audit.

James R. Nobles
Legislative Auditor

Cecile M. Ferkul, CPA, CISA
Deputy Legislative Auditor

Room 140 Centennial Building, 658 Cedar Street, St. Paul, Minnesota 55155-1603 • Phone: 651-296-4708 • Fax: 651-296-4712
E-mail: legislative.auditor@state.mn.us • Web Site: www.auditor.leg.state.mn.us • Minnesota Relay: 1-800-627-3529 or 7-1-1

Table of Contents

Report Summary

Conclusion

The Office of MN.IT Services (MN.IT) generally had adequate internal controls to ensure that it appropriately limited access to its data and protected the mainframe's operating system. MN.IT established expectations for the security controls operating on the mainframe and developed a formal process to evaluate and implement changes. However, MN.IT had some inconsistencies with its internal policies, as noted in the findings in this report.

Key Finding

- The Office of MN.IT Services did not periodically compare its documented mainframe security configuration baseline to the actual mainframe configurations to ensure that any unauthorized variances were resolved. (Finding 1, page 9)

Audit Objective and Scope

The audit objective was to determine whether, as of September 2013, the Office of MN.IT Services had adequate internal controls to: 1) limit the ability to see or modify sensitive mainframe operating system settings and data to appropriate personnel and, 2) to ensure that all modifications to the mainframe operating system were authorized.

Office of MN.IT Services

Mainframe Security Controls

Overview

The State of Minnesota, under the authority of various agencies, has provided centralized mainframe security functions since the installation of the mainframe in the 1980s.[1] Use of the mainframe expanded as computerization became essential to the efficient delivery of critical state services by most state agencies. Utilization peaked in the late 1990s through 2000 when the government functions it supported included:

- Administering medical and cash assistance programs, such as Medical Assistance, Temporary Assistance to Needy Families, and the Supplemental Nutritional Assistance Program.
- Collecting and recording various tax payments.
- Storing information about Minnesota licensed drivers and motor vehicles.
- Maintaining and processing state accounting transactions, including payments to vendors.
- Maintaining human resources records and paying state employees.
- Tracking retirement benefits for state employees.

Over the last decade, a number of agencies moved applications[2] from the centralized mainframe to servers[3] supported by the agencies' information technology staff. For example, the state's 2007 implementation of a new payroll processing system reduced the mainframe's role in personnel and payroll to primarily maintaining reporting functions. Similarly, the state's 2011 implementation of a new accounting system eliminated the mainframe's role in processing and maintaining the state's accounting records. In 2012, when the Department of Revenue completed the consolidation of various tax systems into the GENTAX system, GENTAX eliminated the mainframe from the tax collections processes and relegated it to maintaining historical tax data.

[1] A mainframe is a large computer operated by corporations and government entities to provide a centrally supported environment which processes large quantities of data that is accessed by many users.

[2] An application refers to the coded business logic, data, and supporting system software that allows an end user to perform business functions on a computer.

[3] A server is a midsize computer that provides data and special functions to other computers in a network.

Despite these changes, the state's mainframe still processes significant payments, maintains large volumes of private data, and is used by a substantial number of people and organizations. In 2005, prior to the migration of some widely used applications, there were 20,271 active mainframe accounts.[4] In 2013, there were 13,972 active mainframe accounts. Table 1 shows the distribution of the active 2013 mainframe accounts.

Table 1
Breakdown of Mainframe Accounts
By Type
2013

User Type	Number of Active	Percent
State Employees	3,205	23
County Employees[1]	7,396	53
Contractor, Training, and System	3,371	24
Total	13,972	100%

[1] County employees enter information to support public assistance programs for the Department of Human Services.

Source: Created by Office of the Legislative Auditor from a July 2013 download of user accounts.

While some application and user support occurs within individual agencies, centralizing technical and operational support (such as administering security functions and operating system support) through a centralized computer services office ensures the stability of the computing environment. The Legislature has established and reestablished the responsibility for centralized mainframe services through various legislative actions. Initially, the Department of Administration divided mainframe servers between two of its divisions, Intertechnologies Group and the Office of Technology. In July 2005, the Legislature combined those two divisions and established the Office of Enterprise Technology as a cabinet-level agency. The office, led by the state chief information officer, had two primary responsibilities: 1) set the information technology direction, standards, and policies for the state and manage oversight and compliance of those standards; and, 2) provide common (primarily infrastructure) information technology services to the executive branch and all levels of Minnesota government.

At least one reason for these legislative changes was the identification of weak internal controls in a number of key operational areas for the mainframe, including security. There were various security assessments performed by federal agencies, including the Social Security Administration and the Internal Revenue

[4] An account (also known as a user ID, login ID, or user name) is a mechanism that determines what the person or system is authorized to see, modify, or delete in the application. Accounts are uniquely named to differentiate them from other accounts in the application. The process of "logging in" is when a person or system provides credentials, commonly a password, that when paired with the credentials ensure that the person or system's identity is confirmed.

Service, as well as the Office of Legislative Auditor. In 1999, the Intertechnologies Group engaged a consulting firm to conduct a review that identified significant gaps in the security program. In 2000,[5] 2002,[6] and 2005,[7] the Office of the Legislative Auditor conducted follow up audits that assessed the adequacy of selected mainframe security controls. While there were significant findings, each successive report showed an improvement in the implementation and operation of security controls.

In 2011, the Legislature amended the Office of Enterprise Technology's statute to consolidate under its control the management of all executive branch information technology systems, budgets, services, and resources, significantly increasing the office's responsibilities. The legislation established a state chief information officer who was "responsible for providing or entering into managed services contracts for the provision, improvement, and development of the following information technology systems and services to state agencies: . . . (2) mainframes including system software."[8] In 2013, the office changed its name to the Office of MN.IT Services, commonly referred to as MN.IT.

Just as the agency responsible for the state's information technology services has changed, so has the strategic view of the state's mainframe. MN.IT's 2012 master plan, one of the first reports completed by the newly consolidated office, serves as MN.IT's strategic plan. MN.IT intends the master plan "help guide investments, set consistent priorities, timetables, and goals, and help to leverage new investments for greatest value."[9] It states the following:

> *Our goals are to be an agent of change and help government reinvent itself by identifying next-generation technologies that help state government be faster, more nimble, less bureaucratic and more responsive in the services it provides to citizens, and more able to measure and report on outcomes; and model reform in the reinvention of state IT.*[10]

Mainframes are capable of providing reliable processing and security; however, they carry a high cost. With fewer agencies using the mainframe, the costs

---

[5] Office of the Legislative Auditor, Financial Audit Division Report 00-49, *Department of Administration - Intertechnologies Group System-wide Access to Mainframe Data*, issued October 19, 2000.

[6] Office of the Legislative Auditor, Financial Audit Division Report 02-26, *Department of Administration - Intertechnologies Group System-wide Access to Mainframe Data Follow-up*, issued May 2, 2002.

[7] Office of the Legislative Auditor, Financial Audit Division Report 05-55, *Office of Enterprise Technology Mainframe Security Audit*, issued December 7, 2005.

[8] *Minnesota Statutes* 2013, 16E.016.

[9] Master Plan 2012, Information and Telecommunications Technologies and Services for the State of Minnesota, page 2.

[10] Master Plan 2012, Information and Telecommunications Technologies and Services for the State Minnesota, page 16.

became more difficult to justify. MN.IT has initiated projects to modernize the remaining applications and retire the mainframe. MN.IT intends to continue to work with agencies to ensure that government and citizen data is protected on the mainframe until the modernization projects are complete.

MN.IT's analysis is consistent with the challenges highlighted by William T. Lord, the former U.S. Air Force Chief Information Officer, in a commentary published in 2014 in InformationWeek:[11]

- Around 70 percent of the average IT budget of organization and government agencies goes to legacy software maintenance.
- High operating expenses make it nearly impossible for more organizations and government agencies to invest in new technology.
- The significant risk of failure in software modernization projects is enough to deter attempts to overhaul legacy systems.
- Finding the skilled workforce to support the legacy system is difficult because older workers are retiring and since only 25 percent of colleges still teach legacy programming languages, the investment required to train new workers is very high.

Objective, Scope, and Methodology

The audit objective was to answer the following questions:

- Did the Office of MN.IT Services have adequate controls to limit the ability to see or modify sensitive mainframe operating system settings and data to appropriate personnel?
- Did the Office of MN.IT Services have adequate controls to ensure that all modifications to the mainframe's operating system were authorized?

To answer these questions, we interviewed Office of MN.IT Services' management and staff. We reviewed relevant documentation and used a variety of computer-assisted auditing tools to analyze the mainframe system's security controls.

We conducted this audit in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. To assess security controls, we used:

[11] InformationWeek, *"Breaking the Cycle of Legacy IT Investment,"* March 6, 2014, William T. Lord.

- Department and statewide policies.
- Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, published by the National Institute of Standards and Technology's Computer Security Division.
- *Safeguards and Computer Security Evaluation Matrix CA-ACF2*, published by the Internal Revenue Service.
- Information published by applicable technology vendors, such a Control Associates and IBM, to evaluate select controls.

Conclusion

The Office of MN.IT Services generally had adequate internal controls to ensure that it appropriately limited access to its data and protected the mainframe's operating system. MN.IT established expectations for the security controls operating on the mainframe and developed a formal process to evaluate and implement changes. However, MN.IT had some inconsistencies with its internal policies, as noted in the *Findings and Recommendations* section in this report.

Findings and Recommendations

Finding 1

The Office of MN.IT Services did not periodically compare its documented mainframe security configuration baseline to the actual mainframe configurations to ensure that any unauthorized variances were resolved.

MN.IT's enterprise security configuration management standard states, "Government entities must identify, document, and apply secure baseline configurations based on risk exposure, data classification, compliance requirements, and operating environment that reduce the likelihood or potential impact of known security risks."[12] MN.IT's management generally adopted the Internal Revenue Service's *Safeguards and Computer Security Evaluation Matrix* as the initial configuration baseline for the mainframe system because it provided the most specific data protection guidance for the data stored on the mainframe. For some settings, management also authorized changes to the baseline, either authorizing more lenient or more stringent configurations based on an assessment of operational and security needs.

We tested the mainframe's security configuration and found that it complied with MN.IT's enterprise security configuration management standard requirement that over 90 percent of the actual settings agree to the documented baseline. However, MN.IT had not periodically compared the documented configuration baseline and the actual mainframe settings, as required by the standard. Instead, MN.IT relied on audits conducted by other parties, such as the Internal Revenue Service and the Office of the Legislative Auditor. If it had conducted its own reviews, it could have resolved the following differences we identified:

- MN.IT had not identified any programs as restricted programs.[13] The baseline configuration expects that programs that that do not initiate standard services on the mainframe be restricted because they can circumvent certain security controls.

- MN.IT had not identified certain "maintenance loginids/programs/ libraries" programs as "logged" programs.[14] Because "maintenance loginids/programs/libraries" programs are allowed to execute the programs and circumvent explicit access rules and logging functions, identifying them as logged programs provides a record of when these types of high-risk programs are run. Reviewing the logs can verify the program's authorization.

[12] Enterprise Security Configuration Management Standard, compliance date April 2013.
[13] Safeguards and Computer Security Evaluation Matrix (SCSEM) CA-ACF2, published by the Internal Revenue Service, 2010, TestID ACF2-07.
[14] SCSEM TestID ACF2-22.

- For 176 users, the minimum number of days before the user could change their password was less than five days. While the *Safeguards and Computer Security Evaluation Matrix* suggested a minimum of 15 days,[15] MN.IT management had authorized the minimum to be five days. Minimum password change days prevent users from changing their passwords for a specific time period, reducing the likelihood that a user will change their password back to a recently used password when the system requires a password change.

- For 1,187 accounts, the mainframe would terminate a session in a time greater than the 15 minutes idle time limit in the configuration baseline.[16] For 314 of the 1,187 accounts, no idle time limit was set, and the session would never time out. In addition, 830 state employees' accounts with access to an administrative interface had the idle time limit set to 60 minutes. Per discussions with information technology management, it was determined that this was acceptable because these users would run tasks that may take longer than 15 minutes to run. Management determined that the laptops and desktop computers accessing the mainframe will typically have password based screen savers that would initiate after idle time as a mitigating control. However, MN.IT had not formally documented this assessment nor did they determine if the mitigating control was operating effectively.

In addition to identifying and resolving instances like the ones we found where the actual configuration varied from the baseline configuration, a periodic review would allow staff to identify where the security baseline documentation was not up-to-date with management's expectations and no longer reflected the authorized operating environment.

Recommendations

- *The Office of MN.IT Services should periodically review the mainframe's security configurations to the baseline configuration authorized by MN.IT management and resolve any unauthorized variances.*

- *The Office of MN.IT Services should update baseline configuration documentation for any variances found to be changes to the baseline authorized by MN.IT management.*

[15] SCSEM TestID ACF2-76 value of 15 to a value of 5.
[16] SCSEM TestID ACF2-85.

Finding 2

The Office of MN.IT Services granted access to some audit logs, reporting tools, and sensitive operating system functions but did not implement adequate monitoring controls.

MN.IT granted one user access to modify data directly in the audit log. The audit log data contains all the records of events, such as the view of a logged dataset or a system change, logged by the mainframe. In general, to preserve the audit log's integrity, no users, including administrators, should have access to modify the audit log data.[17] Reports are generated from audit log data for many operational purposes including, security, usage, and monitoring. If the underlying data is modified or deleted then the integrity of those reports is compromised. Per discussions with management, this user required access to modify reporting tools and correct issues with the audit logs. However, management had not implemented sufficient mitigating controls to ensure that the user was only making authorized changes.

In addition, 32 users were granted access to modify the audit reporting tools. While they did not have access to modify audit log data directly, they could modify report criteria to prevent events from displaying in audit reports. This could compromise the intended purpose of the reports by eliminating certain events from subsequent review.

Finally, 17 users who could make changes to key datasets on the mainframe also could initiate an initial program load. The initial program load is a reset of the mainframe to load high-level changes from the test environment to production. When a user can initiate an initial program load and make changes directly to the mainframe, there is a risk that changes promoted into production circumvented MN.IT's required testing and approval for changes.

Recommendations

- *The Office of MN.IT Services should limit access to key datasets and reporting tools on the mainframe to employees who require the access to perform their duties and monitor dataset changes based on the risks to the data.*

- *The Office of MN.IT Services should separate access to certain key datasets from the ability to initiate initial program loads. If the users with the conflicting access cannot be reduced or separated, MN.IT should implement procedures to monitor the users' activity.*

[17] SCSEM TestID ACF2-57.

Finding 3

The Office of MN.IT Services did not adequately monitor some user security events.

MN.IT had not customized reports employees used to monitor security events on the mainframe (such as invalid logins, attempts to access datasets, or create and modify accounts) to better identify unusual or risky events. MN.IT used predefined reports available in the mainframe security software that produced several hundred pages of security events each day. The large volume of events logged increases the risk that employees responsible for reviewing the reports daily might not identify important events or trends. Additionally, the employees responsible for conducting the review had the security access to perform the types of changes contained in the reports. There is a risk of error or noncompliance with internal policies when changes are not reviewed by an independent individual.

By better targeting the types of events included on the report or using analysis tools to facilitate the review, MN.IT could more efficiently and effectively identify and respond to events that pose a risk to the mainframe's operations or data.

Recommendation

- *The Office of MN.IT Services should customize daily security reports or use analytical tools to help employees more efficiently and effectively identify and respond to events that pose risks to the mainframe's operations or data.*

Finding 4

The Office of MN.IT Services did not perform recertification of some highly privileged programs in accordance with its procedures.

Like users, programs can have access to sensitive functions that are usually reserved only for the mainframe's operating system. For example, *supervisor calls* allow a program to perform privileged functions that can impact certain users or the entire system once the program is authorized by the operating system. While MN.IT had an established process to recertify program authorities on an annual basis to ensure that programs have the least privilege they need to operate, it had some weaknesses in that process.

MN.IT last completed a recertification of supervisor calls in 2011. When MN.IT began its 2012 review, staff discovered that the process was not including all supervisor calls. MN.IT staff made the decision to delay the review until they developed a process to provide complete and accurate data. As of October 2013, MN.IT had not completed this recertification.

In February 2013, MN.IT divided the recertification duties for other types of high-level program privileges among five system programmers.[18] Until it was requested as part of our audit in August 2013, MN.IT had not followed up with one of the programs when it had not received the recertification information.

Recommendations

- *The Office of MN.IT Services should complete a full recertification of supervisor calls in the mainframe.*

- *The Office of MN.IT Services should follow-up on recertifications when not received in a timely manner.*

[18] SCSEM Test ID ACF2-40.

April 25, 2014

Mr. James Nobles, Legislative Auditor
Office of the Legislative Auditor
658 Cedar Street
Saint Paul, MN 55155

Dear Mr. Nobles:

I would like to thank your team for the work done on this audit of the MN.IT Services mainframe security controls. We appreciate the time you took to review our process, procedures, and technical controls.

We agree with your overall conclusion: The Office of MN.IT Services (MN.IT) generally has adequate internal controls but we could do more to regularly review our secure operating environment against industry recommendations. However, we want to emphasize that the mainframe is one of the State's most secure and mature operating environments. We certainly need to be vigilant to changes, as this report has pointed out, but the mainframe's operations and procedures are some of the safest and most thorough within the State. It is important to emphasize that, as your office well knows, the security challenges the State faces today go well beyond legacy mainframe security services.

For context, MN.IT Services is in the process of consolidating security resources into enterprise and line of business teams under single management (scheduled to occur in FY2015). This will bring the minimum appropriate security resources to all applicable agencies, boards, and commissions and change how we address the issues raised in this and future OLA reports.

What follows is MN.IT's response to the findings in the OLA report.

I look forward to working with policy makers and executive branch leaders to bridge the State's current security challenges and risks.

Sincerely,

Carolyn Parnell
State Chief Information Officer

MN.IT Services
658 Cedar Street, Saint Paul MN 55155
mn.gov/mnit

Finding 1

The Office of MN.IT Services did not periodically compare its documented mainframe security configuration baseline to the actual mainframe configurations to ensure that any unauthorized variances were resolved.

OLA Recommendation

- *The Office of MN.IT Services should periodically review the mainframe's security configurations to the baseline configuration authorized by MN.IT management and resolve any unauthorized variances.*
- *The Office of MN.IT Services should update baseline configuration documentation for any variances found to be changes to the baseline authorized by MN.IT management.*

MN.IT Response

We concur with both the finding and recommendations. MN.IT Services will audit the mainframe baseline security configuration in November of each year. This review will ensure that all configuration changes were authorized and followed established change control procedures. When changes are authorized, MN.IT will continuously update its baseline configuration records.
Person Responsible: Debra Stafford
Estimated Completion Date: 12/31/2014

Finding 2

The Office of MN.IT Services granted access to some audit logs, reporting tools, and sensitive operating system functions but did not implement adequate monitoring controls.

OLA Recommendations

- *The Office of MN.IT Services should limit access to key datasets and reporting tools on the mainframe to employees who require the access to perform their duties and monitor dataset changes based on the risks to the data.*
- *The Office of MN.IT Services should separate access to certain key datasets from the ability to initiate initial program loads. If the users with the conflicting access cannot be reduced or separated, MN.IT should implement procedures to monitor the users' activity.*

MN.IT Response:

We concur with the finding and recommendations. MN.IT Services will work to add to its current process for reviewing access to key datasets, expanding our scope to include certain datasets and resources identified in the audit. MN.IT will also explore options to separate duties and provide additional monitoring of individuals that can perform initial program loads on the mainframe.
Person Responsible: Debra Stafford
Estimated Completion Date: 12/31/2014

MN.IT Services
658 Cedar Street, Saint Paul MN 55155
mn.gov/mnit

Finding 3

The Office of MN.IT Services did not adequately monitor some user security events.

OLA Recommendations

The Office of MN.IT Services should customize daily security reports or use analytical tools to help employees more efficiently and effectively identify and respond to events that pose risks to the mainframe's operations or data.

MN.IT Response

We concur with the recommendation. MN.IT Services reviews ACF2 reports on a daily basis. MN.IT staff will work to automate ACF2 report monitoring in order to hone in on high risk events as they occur, rather than through the review of reports after the fact.

Person Responsible: Debra Stafford

Estimated Completion Date: 12/31/2015

Finding 4

The Office of MN.IT Services did not perform recertifications of some highly privileged programs in accordance with its procedures.

OLA Recommendation

- The Office of MN.IT Services should complete a full recertification of supervisor calls in the mainframe.
- The Office of MN.IT Services should follow-up-up on recertifications when not received in a timely manner.

MN.IT Response

We acknowledge that one of thirty-five recertification processes was not completed in a timely manner. Mitigating controls have been implemented to address this finding.

Of the 35 mainframe access certifications conducted annually, approximately 3,320 accounts were certified with 540 letters sent to management for verification and signature in 2013. Recertification of the supervisor calls was completed in 2011 and then postponed to allow staff to research and implement a more comprehensive process. Supervisor call certification resumed in March 2014, with a more comprehensive process, and will be completed again at the annual certification time in November 2014.

Person Responsible: Debra Stafford

Estimated Completion Date: 12/31/2014