Office of MNIT Services

Information Technology Change Management Controls

January through June 2017

January 10, 2018
REPORT 18-01

Financial Audit Division

OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

Office of the Legislative Auditor
Financial Audit Division

The Financial Audit Division at the Office of the Legislative Auditor (OLA) performs three types of audits of entities within the state's executive and judicial branches:

- **Financial Statement** audits determine whether an entity has prepared its Comprehensive Annual Financial Report in accordance with governmental accounting principles. The division provides audit opinions on the financial reports for the State of Minnesota, the state's three large public pension plans, and the Minnesota Sports Facilities Authority.

- **Federal Grant Compliance** audits determine whether the state has complied with federal requirements for many of its largest federal programs. Often called the *Single Audit*, the federal government requires these audits as a condition of receiving federal grants.

- **Internal Controls and Legal Compliance** audits determine whether an entity has internal controls to effectively manage the risks of its financial operations and whether it has complied with legal compliance requirements chosen for testing.

The Financial Audit Division has a staff of about 35 auditors, many of whom are licensed CPAs and hold other certifications. The division conducts its audits in accordance with *Government Auditing Standards* established by the Comptroller General of the United States.

One requirement of the audit standards is a periodic review of the division's system of quality control by audit peers from across the country. The division's most recent peer review report is available at: www.auditor.leg.state.mn.us/fad/pdf/fadpeer.pdf

---

OLA also has a **Program Evaluation Division** that evaluates topics periodically selected by members of the Legislative Audit Commission.

In addition, OLA may conduct a **Special Review** 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 to determine what additional action, if any, OLA should take.

Photo provided by the Minnesota Department of Administration with recolorization done by OLA.
(https://www.flickr.com/photos/139366343@N07/25811929076/in/album-72157663671520964/)
Creative Commons License: https://creativecommons.org/licenses/by/2.0/legalcode

OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA • James Nobles, Legislative Auditor

January 10, 2018

Senator Mary Kiffmeyer, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Thomas Baden, Commissioner and Chief Information Officer
Office of MNIT Services

This report presents the results of our audit of the Office of MNIT Services' information technology change management controls as of June 2017. The objectives of this audit were to determine if the Office of MNIT Services had adequate change management processes and controls to provide reasonable assurance that changes complied with its established process.

We discussed the results of the audit with the office's staff at an exit conference on December 20, 2017. This audit was conducted by Michael Anderson, CPA, CISA (Information Technology Audit Director) and Michael Fenton, CISA (Information Technology Audit Coordinator).

We received the full cooperation of the office's staff while performing this audit.

James Nobles
Legislative Auditor

Christopher Buse
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 • Website: www.auditor.leg.state.mn.us • Minnesota Relay: 1-800-627-3529 or 7-1-1


THE GREAT SEAL OF THE STATE OF MINNESOTA
L'ETOILE DU NORD
1858

Table of Contents


THE GREAT SEAL OF THE STATE OF MINNESOTA
L'ETOILE DU NORD
1858

Report Summary

Background

Changes to government systems are necessary to help agencies meet evolving business needs, address new compliance requirements, and fix security vulnerabilities. Closely managing changes is extremely important because all changes pose risks to the stability of highly-complex systems and the availability of critical government services.

Organizations that manage complex technology systems typically adopt strict change management processes. These processes help technology leaders understand and manage risk while making carefully planned changes to systems. The overarching goal of change management is to minimize the impact of change-related incidents.

Conclusion

MNIT Services had generally adequate change management controls. The agency had adequate policies and standards, and changes that we tested followed those standards. However, disparate change management software products and processes may increase the likelihood of change-related failures and prolonged service outages. We also found that MNIT lacks key controls to detect unauthorized changes.

Audit Findings

- Disparate change management software products and processes increase the likelihood of change-related failures and prolonged service outages. (Finding 1, page 5)

- MNIT lacks key controls to detect unauthorized changes. (Finding 2, page 5)


THE GREAT SEAL OF THE STATE OF MINNESOTA
L'ETOILE DU NORD
1858

Background

Changes to government systems are necessary to help agencies meet evolving business needs, address new compliance requirements, and fix security vulnerabilities. Closely managing changes is extremely important because all changes pose risks to the stability of highly-complex systems and the availability of critical government services. To illustrate, in August 2015, the state's e-mail system was offline for 23 hours because the service provider made an unauthorized change.

Organizations that manage large technology systems typically adopt strict change management processes. These processes help technology leaders understand and manage risk while making carefully planned changes to systems. The overarching goal of change management is to minimize the impact of change-related incidents.

MNIT Services has comprehensive change management policies and standards, which closely align with industry best practices.[1] These standards require formal documentation for all proposed changes, internal reviews and testing. MNIT standards also require changes to go through a Change Advisory Board, which approves the implementation date and time of all changes.

Objectives, Scope, and Methodology

Our audit examined change management controls for the period from January 1, 2017, through June 30, 2017. We planned our work to answer the following questions:

- Did MNIT Services have adequate change management processes?
- Did MNIT Services have controls to provide reasonable assurance that changes complied with its established process, including:
    - Preparation of formal change documentation;
    - Assessment of potential change risks; and
    - Review, testing, and approval of changes prior to implementation.

To meet these objectives, we interviewed MNIT staff to gain an understanding of change management policies and standards. We also tested changes at four MNIT field offices and changes made by enterprise service delivery teams, using MNIT policies and standards as criteria.

We conducted the audit in accordance with generally accepted government auditing standards.[2] Those standards require that we plan and perform the audit to

[1] Information Technology Infrastructure Library V3, Change Management.

[2] U.S. Government Accountability Office, *Government Auditing Standards*, December 2011.

obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives.

Conclusion

MNIT Services had generally adequate change management controls. The agency had adequate policies and standards, and changes that we tested followed those standards. However, disparate change management software products and processes may increase the likelihood of change-related failures and prolonged service outages. We also found that MNIT lacks key controls to detect unauthorized changes.

The following *Findings and Recommendations* section provides further explanation about the exceptions noted above.

Findings and Recommendations

Disparate change management software products and processes increase the likelihood of change-related failures and prolonged service outages. **Finding 1**

MNIT Services has comprehensive change management policies and standards. Implementation of those policies and standards occurs in numerous agency offices, with varying levels of rigor and multiple change management software products. A decentralized change management approach made sense when agency offices controlled their entire technology environment. However, today many agency business systems harness servers, storage, and other technologies that are managed by enterprise teams. With a blended service delivery strategy, it is vital to more closely integrate change management processes because modifications made by any team can have unanticipated and far-reaching consequences on other teams.

MNIT has made some progress consolidating change advisory boards. However, with multiple change management software products, MNIT currently has no single source of reliable information to quickly diagnose and resolve problems. Time is of the essence when critical system outages occur. One of the first questions that technology leaders ask during an outage is: What changed? To answer that question, leaders turn to change management software products, which contain detailed information about all changes that were approved by a Change Advisory Board. Particularly for critical system outages that occur after normal business hours, not having a single source of reliable information to quickly diagnose and resolve problems may result in prolonged system outages.

Recommendation

- *MNIT Services should work to more closely integrate disparate change management processes and software products.*

MNIT lacks key controls to detect unauthorized changes. **Finding 2**

Change management processes are an important control to prevent disruptions to critical government services. However, it is equally important to have detective controls to identify situations where employees circumvent established change processes.

Configuration compliance software products help organizations monitor technology environments for unauthorized changes. These software products regularly scan environments and compare the results to known baselines. Departures from known baselines may indicate changes that circumvented established change management processes. MNIT recently started piloting configuration compliance software products in several technology environments.

However, most MNIT environments lack detective controls to identify unauthorized changes.

Recommendation

- *MNIT Services should deploy specialized software to improve its ability to detect unauthorized changes.*

MINNESOTA IT SERVICES

Minnesota IT Services
658 Cedar Street
St. Paul, MN 55155

January 8, 2018

Mr. James R. Nobles
Legislative Auditor
Office of the Legislative Auditor
658 Cedar Street, Suite 140
St. Paul, Minnesota 55155

Dear Mr. Nobles,

I would like to begin by thanking your team for the work done on this audit of MN.IT Information Technology Change Management Controls. We appreciate your team's effort and time in reviewing our standards and policies around change management, talking to many staff, and reviewing our processes in action through the executive branch. Change management is an import control that helps MN.IT ensure uptime of critical applications, as well as the security of the applications we support for our agency business partners.

Since the 2011 IT consolidation legislation was enacted, MN.IT has worked toward consolidating the change management processes and procedures throughout the executive branch. As your report points out, MN.IT does have a comprehensive set of policies and standards around change management and has made some progress in consolidating some of the larger change management organizations. But as the report also points out in Finding 1, there is still more work to be done. MN.IT plans to continue to consolidate the other agencies under the MN.IT Enterprise Change Management organization to mitigate the issues presented when change happens without the greater organization having visibility and understanding.

MN.IT also acknowledge the issues raised in Finding 2 related to the lack of key controls to detect unauthorized changes. This is an area where we have put significant effort into planning, and the cost to implement this plan has been part of the cybersecurity budget request put forward in both the 2016 and 2017 legislative sessions. Specifically, MN.IT requested funding during those session for the purchase and implementation of tools to detect and prevent unauthorized changes. MN.IT has policy prohibiting unauthorized changes and has reprimanded staff that break that policy. But without this funding, we have not been able to acquire and implement these preventative and detective controls, putting mission-critical state applications at risk of unauthorized changes.

Thank you once again for the outstanding work on this extremely important topic. Nothing is more important to Minnesota IT Services than protecting the security of data and ensuring the ongoing availability of critical government services.

Sincerely,

Thomas Baden,
Commissioner Minnesota IT Services

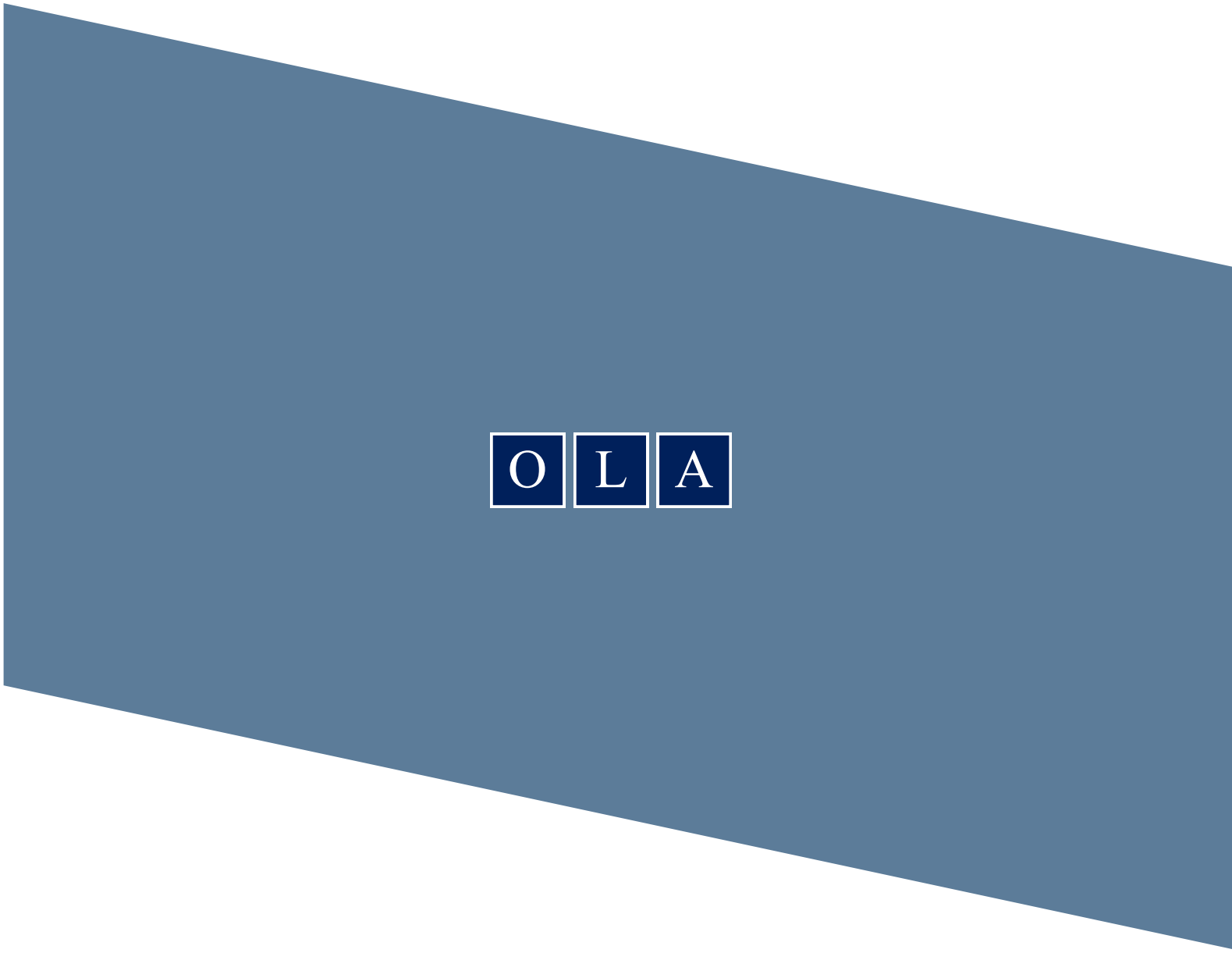

THE GREAT SEAL OF THE STATE OF MINNESOTA
L'ETOILE DU NORD
1858

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 email 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 7-1-1 or 1-800-627-3529.

Printed on Recycled Paper



OFFICE OF THE LEGISLATIVE AUDITOR
CENTENNIAL OFFICE BUILDING – SUITE 140
658 CEDAR STREET – SAINT PAUL, MN 55155