Disaster Recovery Strategies for Critical IT Systems

Information Technology Audit

September 2022

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.

Photo provided by the Minnesota Department of Administration with recolorization done by OLA.
(https://www.flickr.com/photos/139366343@N07/25811929076/in/album-72157663671520964/)

OLA **OFFICE OF THE LEGISLATIVE AUDITOR**
STATE OF MINNESOTA • Judy Randall, Legislative Auditor

September 29, 2022

Members
Legislative Audit Commission

Tarek Tomes, Commissioner and State Chief Information Officer
Minnesota IT Services

Jim Schowalter, Commissioner, Department of Management and Budget,
and Chair of the Continuity Policy Coordination Sub-Cabinet

This report presents the results of our information technology audit of Minnesota IT Service's disaster recovery oversight and system restoration capabilities. The objectives of this audit were to determine if Minnesota IT Services and selected state agencies had adequate plans in place to minimize the recovery time of key information technology systems in the event of major disruption, and review centralized management and oversight of disaster recovery planning.

We have omitted certain technical details and one audit issue from this report in the interest of protecting information security. We discussed specific issues or gaps noted within the disaster recovery plans with MNIT and the related agency.

This audit was conducted by Mark Mathison (IT Audit Director), Joe Sass (IT Audit Coordinator), and auditors Tyler Billig and Zachary Kempen.

We received the full cooperation of agency personnel while performing this audit.

Sincerely,

Lori Leysen

Mark Mathison

Lori Leysen, CPA
Deputy Legislative Auditor

Mark Mathison, CISA, CISSP, CPA (Inactive)
IT Audit Director

Cc: Nate Clark, Chief Executive Officer, MNsure
Jodi Harpstead, Commissioner, Minnesota Department of Human Services
Lee Ho, Interim Commissioner, Minnesota Department of Revenue

OLA

Table of Contents

OLA

Introduction

Sudden, unplanned events can occur that cause damage or loss to a state agency's information system. Whether it is a natural disaster, fire, ransomware, virus, power failure, or other service disruption, these events can compromise an agency's ability to provide critical functions or services for an extended period. Should an event happen that results in the disruption of government operations, the state would still need to provide public safety services; make pension payments; deposit tax revenues; provide aid to schools, local governments, and benefit enrollees; and provide many other important services. In this type of situation, state agencies would need to invoke their business continuity of operations plans (COOPs) and information technology disaster recovery (IT DR) plans.[1]

Disaster Recovery Plan

A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities.

— National Institute of Standards and Technology (NIST)

Over the past fifty years, Minnesota governors have issued executive orders mandating agencies to prepare plans and instructions for continuing government services in the event of a disaster.[2] The most current order—Executive Order 19-23—provides for the continuity of essential state functions and critical priority services during any incident, emergency, or disaster.[3] Governor Tim Walz's executive order sets forth requirements for state agencies to develop COOPs and outlines the contents for those plans. The order further directs Minnesota IT Services (MNIT) to "establish information technology disaster recovery plans that align with the priorities and recovery timelines of agency priority services to ensure the State is adequately managing the risk of system and service interruptions."[4]

The Office of the Legislative Auditor (OLA) conducted this selected scope audit to determine whether MNIT and selected state agencies had IT DR plans to minimize the recovery time of key systems and applications if a major disruptive event or disaster were to occur. For our audit, we reviewed MNIT's centralized disaster recovery planning and oversight activities. We also selected four of the state's larger information systems and evaluated what steps MNIT has taken to prepare itself and its partnering

[1] A *business continuity of operations plan* (COOP) documents the procedures for sustaining an organization's business processes during and after a significant disruption to business operations, including disruptions to an IT system. An *information technology disaster recovery* (IT DR) plan is a written plan for recovering information systems in response to a major hardware or software failure or facility destruction. Whereas COOP is the process to recover the business, IT DR is about recovering the entity's IT infrastructure.

[2] See the Appendix on page 21.

[3] State of Minnesota Executive Order 19-23, "Directing the Development and Maintenance of the Minnesota Continuity of Government Plan and Agency Continuity of Operations Plans," April 4, 2019.

[4] *Ibid*.

agencies for a disaster. Our work reviewed MNIT’s oversight and management, and the status of each system’s disaster recovery planning efforts, as of November 2021.

The systems that we reviewed as part of this audit include:

- Medicaid Management Information System (MMIS), owned by the Department of Human Services.

- Minnesota Eligibility Technology System (METS), co-owned by the Department of Human Services and MNsure.

- Integrated Tax System (also referred to as GenTax), owned by the Department of Revenue.

- A fourth priority system in which activities could be interrupted temporarily, but must be recovered within the first week of any interruption.[5]

These information systems represent a variety of technical platforms within the state ecosystem and support the operation of key government services. An extended period of unavailability for any of these systems would likely have a serious impact on state and agency services.

In the context of our audit, we refer to a “disaster” as a significant incident that requires the activation of a system’s IT DR plan. These incidents can take many forms, such as damaged or malfunctioning data center infrastructure, fire, flood, tornado, or ransomware. At its core, a disaster is any incident that prevents normal system functions from occurring and requires restoration of the system within a secondary or alternative location.

[5] Due to weaknesses with the disaster recovery plan for this system, and in an effort to protect its security, OLA is not naming the system or responsible agency in this public report.

Report Summary

Conclusions

In the event of a disaster, Minnesota IT Services (MNIT) and state agencies are generally prepared to restore three of the four information technology systems that we reviewed. MNIT has developed disaster recovery plans for each system and has demonstrated its preparedness to recover three of the systems through various forms of plan testing and exercises. We believe that, in the event of a disaster, MNIT and its partnering agencies are prepared to recover the Medicaid Management Information System (MMIS), the Minnesota Eligibility Technology System (METS), and the Integrated Tax System (GenTax). However, we found one priority system in which the disaster recovery planning efforts did not follow best practices. Inadequate plans, combined with a lack of testing, led us to conclude that MNIT and its partnering agency are not prepared to restore this system within the desired timeframe.

We further concluded that MNIT has centralized policies and procedures to provide effective oversight and management of disaster recovery planning efforts. However, we noted that some of MNIT's manual oversight processes are prone to human error and inefficiencies.

The results of our audit apply only to the four systems that we reviewed and do not indicate the overall status of disaster recovery for MNIT's broad portfolio of nearly 2,800 information systems and applications.

Findings

Finding 1. MNIT's manual disaster recovery tracking process is prone to human error and lacks functionality. (p. 14)

Finding 2. MNIT and its partnering agency are not adequately prepared to restore one priority system within the desired timeframe. (p. 17)

OLA

Background

Minnesota Government Continuity Governance Framework and Responsibilities

Recognizing the need for contingency planning, Minnesota governors have routinely signed executive orders that mandated agencies to prepare plans and instructions for continuing government services in the event of a disaster.[6] Executive Order 19-23, issued by Governor Tim Walz, is the current such order that addresses the continuity of essential state functions and the provision of critical priority services during any incident, emergency, or disaster.[7]

Executive Order 19-23 preserves the Continuity Policy Coordination Sub-Cabinet (Sub-Cabinet), a governance body responsible for developing and maintaining a continuity of government framework and overseeing agency continuity of operations planning. The Sub-Cabinet consists of the Commissioner, or designees, of the Department of Management and Budget (MMB), the Department of Public Safety, the Department of Administration, and Minnesota IT Services (MNIT). The order designated MMB's commissioner as the chair of the Sub-Cabinet and the lead agency for continuity planning and program coordination.

The Sub-Cabinet has delegated certain responsibilities to a State Agency Continuity Steering Committee (Steering Committee), a working group under the Sub-Cabinet. The Steering Committee is tasked with providing leadership and direction to state executive branch agencies. To this end, members of the Steering Committee create business continuity of operations plans (COOPs) and information technology disaster recovery (IT DR) plan templates that can be used by agencies. They also offer guidance and consultation to agencies as needed.

Executive Order 19-23 requires each state entity to develop a COOP and outlines what should be included in the plan. Finally, the order requires MNIT to establish IT DR plans that align with agencies' priority services.

The continuity governance framework and responsibilities are articulated in Exhibit 1.

[6] See the Appendix on page 21.

[7] State of Minnesota Executive Order 19-23, "Directing the Development and Maintenance of the Minnesota Continuity of Government Plan and Agency Continuity of Operations Plans," April 4, 2019.

Exhibit 1: State of Minnesota Continuity Governance Framework

Continuity Policy Coordination Sub-Cabinet

Role: Develop and maintain a framework for the state continuity of government (COG) plan and oversee agency COOP planning
Members: Department of Management and Budget, Department of Public Safety, Department of Administration, and MNIT Services

Department of Management and Budget	Department of Public Safety	Department of Administration	MNIT Services
Chair of Sub-Cabinet Lead for continuity planning and program coordination Direct response during emergencies impacting state services Lead workforce planning Maintain priority services lists Direct employee reassignments during emergencies	Provide emergency response Align efforts with emergency management functions	Coordinate alternative facilities and facility contracts Lead emergency procurement and contracting	Establish plans for the continuation and recovery of technology that align with agency priority services

State Agency Continuity Steering Committee

Role: Support the Sub-Cabinet and provide leadership and direction to state executive branch agencies

Members: Continuity Leads from the Department of Management and Budget, Department of Public Safety, Department of Administration, and MNIT Services

State Executive Branch Agencies

Commissioner/Department Head
- Commit resources to develop and maintain plans and procedures

Continuity Coordinator
- Coordinate development of COOPs and support of the state COG plan

Managers/Supervisors
- Establish recovery timelines for services
- Develop and maintain plans to recover services
- Assign employees to response and recovery teams
- Assign employees to alternative work sites
- Exercise and train employees on plans and procedures

Employees
- Update their personal contact information
- Know their response and recovery roles
- Know their alternative work sites
- Participate in training and exercises

Source: Office of the Legislative Auditor, based on information received from MMB and MNIT.

Information Technology Contingency Planning

To help fulfill its mission, MNIT has a centralized team of three staff who are dedicated to statewide disaster recovery efforts. This centralized disaster recovery team assists with the administration of policies, standards, and guidelines. They also track and coordinate the testing plans for approximately 2,800 information systems and applications across the executive branch. MNIT staff working within each agency are responsible for the development and ongoing maintenance of the specific IT DR plans for their respective agency.

Best practices prescribe the process to develop and maintain an effective IT DR plan. Responsibility for the planning process generally falls under the role of an information system contingency plan coordinator. This coordinator, who would typically be a MNIT staff person, develops the planning process in cooperation with other MNIT technical support managers, agency leaders responsible for the business processes supported by the system, and the respective agency business continuity coordinator. Exhibit 2 illustrates the seven common steps within the contingency planning process.

Exhibit 2: Seven Steps for Information Technology Contingency Planning

Develop Contingency Planning Policy	• Identify statutory or regulatory requirements • Develop IT contingency planning policy statement • Publish policy
Conduct Business Impact Analysis	• Determine impact of a system outage • Identify statutory or regulatory requirements • Identify resource requirements • Identify recovery priorities for system
Identify Preventive Controls	• Identify controls • Implement controls • Maintain controls
Create Recovery Strategies	• Define data backup and recovery methods • Identify roles and responsibilities • Identify alternative sites • Identify equipment and cost considerations • Integrate into system architecture
Develop Disaster Recovery Plan	• Document recovery strategy
Plan Training, Testing, and Exercises	• Train personnel • Test and exercise the recovery plan
Plan Maintenance	• Review and update plan • Coordinate with internal/external organizations • Control plan distribution • Document changes

Source: Office of the Legislative Auditor, adapted from U.S. National Institute of Standards and Technology, Special Publication 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*, November 2010.

Priorities and Recovery Timelines

Effective contingency planning begins by subjecting each information system to a business impact analysis (BIA).[8] The purpose of the BIA is to correlate specific IT components with the critical processes that they support and, based on that information, to characterize the consequences of a disruption to the components. Results from the BIA should be incorporated into the COOPs and IT DR plans. Agency staff should perform BIAs early and throughout the system lifecycle.[9] This facilitates prioritizing systems based on the impact level, so that recovery strategies can minimize potential loss.

Prioritizing information systems can be complex, as systems may support multiple business processes, resulting in different perspectives on the importance of a system. This complexity is compounded when an entire state government with numerous information systems must establish priorities. What may be important to one division of one agency may not be the most critical system for the state as a whole. For this reason, information system continuity planners must work with program managers and agency leadership to determine the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO) for a given information system. The IT DR plans and strategies are then developed to meet these objectives.

Recovery Time Objective (RTO)

The overall length of time an information system's components can be in the recovery phase before negatively impacting the organization's mission or business processes.

Recovery Point Objective (RPO)

The point in time, prior to a disruption or system outage, to which data must be recovered after an outage.

— National Institute of Standards and Technology (NIST)

To assist with prioritization, the State Agency Continuity Steering Committee has set forth four categories that group state services by RTO:

Priority 1 – Activities that must remain uninterrupted or must be recovered within 24 hours.

Priority 2 – Activities that can be interrupted temporarily or might be periodic in nature but must be recovered within the first week of interruption.

[8] U.S. National Institute of Standards and Technology, Special Publication 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*, November 2010, section 3.2, pp. 15-19.

[9] The system development lifecycle (SDLC) refers to the full scope of activities conducted by information system owners associated with a system during its lifespan. The lifecycle begins with *Initiation* and ends with *Disposition*. Although contingency planning is associated with activities occurring mostly in the *Operation/Maintenance* phase, identification and integration of contingency strategies at all phases of the information system lifecycle allow the owner to build layered protection against risks and assist implementation of effective recovery strategies early in the system development.

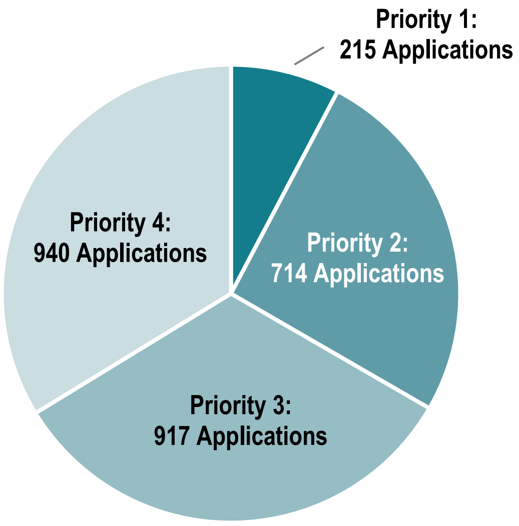
Priority 3 – Activities that can be interrupted temporarily but must be recovered within the first 30 days of interruption.

Priority 4 – Activities that can be suspended for at least 30 days and potentially for the duration of the interruption.

When developing a disaster recovery strategy, technical staff must work with business staff to understand the need for system availability and balance it with the risk and likelihood of disruption. Typically, recovery strategies that support short RTO and RPO are costly. Recovery strategies designed to minimize or eliminate downtime using load balancing across data centers, redundancy and data mirroring between data centers, and backup to alternative sites require more complex planning, technical infrastructure, maintenance, and testing. Lower priority systems—those with longer RTO and RPO—can use less expensive options because the business has indicated that they can tolerate longer downtimes for recovery and restoration of data.

MNIT maintains a portfolio that contains a variety of information on the roughly 2,800 information systems and applications that it oversees or supports on behalf of state agencies. To help manage recovery efforts, MNIT records the priority and RTO of each system. As represented in Exhibit 3, MNIT's portfolio contains over 200 systems that are categorized as supporting Priority 1 services, or needing to be restored within 24 hours from the time of a disaster. An approximate 700 additional systems support Priority 2 services, with RTOs of a week or less.

Exhibit 3: MNIT's Portfolio of Systems by Recovery Priority



Source: Office of the Legislative Auditor, analysis of MNIT systems and application data, as of September 17, 2021.

Audit Scope, Objectives, Methodology, and Criteria

The Office of the Legislative Auditor (OLA) conducted this selected scope audit to determine whether Minnesota IT Services (MNIT) and selected agencies had sufficient information technology disaster recovery (IT DR) plans in place to minimize the recovery time of key systems and applications if a major disruptive event or disaster were to occur. Using risk assessment processes and professional judgement, we selected 4 of the nearly 2,800 information systems and applications under MNIT's purview and evaluated what steps MNIT has taken to prepare itself and its partnering agencies for a disaster.

We sought to understand MNIT's involvement in agency information technology disaster recovery planning through its centralized efforts to provide oversight, tracking, guidance, and assistance in staging disaster recovery exercises. This work helped us answer the question:

> **Does MNIT's centralized disaster recovery team provide effective management and oversight of disaster recovery planning?**

To answer our question on effective management and oversight, we met with MNIT's centralized disaster recovery team, reviewed materials such as IT DR plan templates, and examined MNIT's tools for planning and tracking disaster recovery plans.

Beyond the centralized control environment, we further conducted audit steps to answer the question:

> **Are MNIT and selected state agencies prepared to restore significant information technology systems in the event of a disaster?**

The four significant systems in our review included:

- Medicaid Management Information System (MMIS), owned by the Department of Human Services.
- Minnesota Eligibility Technology System (METS), co-owned by the Department of Human Services and MNsure.
- Integrated Tax System (also referred to as GenTax), owned by the Department of Revenue.
- A fourth priority system in which activities could be interrupted temporarily, but must be recovered within the first week of any interruption.[10]

[10] Due to weaknesses with the disaster recovery plan for this system, and in an effort to protect its security, OLA is not naming the system or responsible agency in this public report.

OLA selected these systems for review due to their differing underlying technologies, supporting agencies, state and federal requirements, and the potential impact to state government and the citizens of Minnesota if unavailable.

For each system, OLA designed its work to address the following questions:

- Does an information technology disaster recovery plan exist?
- Do the information technology disaster recovery plans contain appropriate information and procedures to restore or rebuild the systems?
- Have MNIT and the agencies tested their information technology disaster recovery plans?

To answer these questions, OLA interviewed staff involved in developing and exercising these four systems' IT DR plans, and reviewed those plans and other associated documentation. We tested the plans for completeness and for consistency with the recovery objectives outlined in each agency's respective COOP. Finally, we evaluated how these systems aligned with enterprise oversight and policies. Our work reviewed MNIT's oversight and management, and the status of each system's disaster recovery planning efforts, as of November 2021.

We conducted this information technology performance audit in accordance with generally accepted government auditing standards.[11] 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.

Using applicable executive orders, agency policies and standards, and the National Institute of Standards and Technology (NIST) industry best practices, we tested the adherence to policies and best practices and the potential effectiveness of the disaster recovery plans for the sampled systems, ultimately concluding whether the systems could be recovered.[12]

Because we selected a nonstatistical sample—selecting just 4 information systems from the overall population of nearly 2,800 information systems and applications—the results of our testing cannot be extrapolated. As such, our conclusions are relevant to the selected systems only and do not represent the ability to recover other systems for which MNIT is responsible.

[11] Comptroller General of the United States, Government Accountability Office, *Government Auditing Standards* (Washington, DC, December 2018).

[12] As a basis to define industry best practices, we used the U.S. National Institute of Standards and Technology, Special Publication 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*, November 2010; U.S. National Institute of Standards and Technology, Special Publication, 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, September 2006; and ISACA's COBIT 2019, a framework for the governance and management of information and technology.

Audit Testing

Management and Oversight of Disaster Recovery Planning

MNIT has established an Information Technology Disaster Recovery Planning Policy and an Information Technology Disaster Recovery Planning Standard outlining disaster recovery planning actions and requirements.[13] The Disaster Recovery Planning Standard requires that disaster recovery plans "must be developed and maintained for critical systems"—those supporting Priority 1 and 2 services. The standard also lays out the requirements for information technology disaster recovery planning activities, including plan development, distribution, review, training, and testing; data backup; and alternative site recovery.

> Information technology disaster recovery (IT DR) plans must be in place that align with the priorities and recovery timelines of state agency critical priority services to ensure the State of Minnesota is adequately managing the risk of system and service interruptions.
>
> **— MNIT Information Technology Disaster Recovery Planning Policy Statement**

MNIT's centralized disaster recovery team, working as part of the State Agency Continuity Steering Committee, has developed an information technology disaster recovery (IT DR) plan template. This template provides MNIT information system contingency plan coordinators at each agency with guidance, an outline, and basic expectations for a system's IT DR plan that meets best practices and the requirements defined in MNIT's Information Technology Disaster Recovery Planning Standard. As MNIT staff at each agency complete or update their respective IT DR plans, MNIT's central disaster recovery coordinator provides a basic review of the plan to ensure that components of the template have been completed. The MNIT central disaster recovery coordinator then seeks to obtain formal approvals of the IT DR plans from the MNIT technical system owner(s) and agency business owner(s) who are responsible for the system and the services that it supports.

MNIT's centralized disaster recovery team manually tracks the status of IT DR plans and testing activities on a spreadsheet. Organized by priority level, the spreadsheet contains various data points for MNIT's portfolio of almost 2,800 information systems and applications. In our review of the disaster recovery tracking spreadsheet and sampled systems, we noted discrepancies within MNIT's spreadsheet data.

[13] Minnesota Information Technology Services, *Information Technology Disaster Recovery Planning Policy*, version 1.4, approved March 10, 2020; and Minnesota Information Technology Services, *Information Technology Disaster Recovery Planning Standard*, version 1.4, approved March 10, 2020.

FINDING 1

MNIT's manual disaster recovery tracking process is prone to human error and lacks functionality.

While a reasonable first step in cataloging MNIT's complex software environment, MNIT's disaster recovery tracking spreadsheet is prone to human error and lacks functionality to fully support enterprise-wide disaster recovery efforts. For example, two of the four IT DR plans that we examined had a Recovery Time Objective (RTO) within the tracking spreadsheets that did not match the RTO identified within the respective IT DR plans. MNIT's spreadsheet also had missing data elements used to indicate the receipt of the Department of Revenue's GenTax IT DR plan. When asked, MNIT officials told us that they had indeed received the plan, but it was not in the newest MNIT template format. Because this spreadsheet data is utilized to produce reports for MNIT senior leadership, MNIT's reporting would not accurately reflect the current level of preparedness. Having accurate information during a significant disaster would also be essential for managing recovery efforts.

Tracking disaster recovery information in a single spreadsheet for the nearly 2,800 information systems and applications can pose other challenges. First, utilizing a single spreadsheet makes it difficult for more than one person to update information. MNIT may receive more accurate and up-to-date information if MNIT staff at agencies were able to enter plan information directly, rather than relaying the information to a centralized resource for input. Unfortunately, this is not feasible with a single spreadsheet, which presents unique challenges when having multiple simultaneous editors and would require broad access authority across many staff and agencies. Second, because a spreadsheet does not allow for tracking changes, insight into what data values were entered, updated, or removed, when and by whom, would not be available.

MNIT could benefit from using business continuity management and disaster recovery planning software. With a proven software solution, MNIT could build and manage business impact analyses, risk assessments, and IT DR plans. MNIT may also be able to develop coordinated recovery strategies, stage and exercise those disaster recovery strategies, and respond in the event of an actual disaster. Business continuity management and disaster recovery planning software could also provide reporting capabilities to help equip agency leaders and decision makers with accurate and up-to-date information. MNIT's centralized disaster recovery team and supported agencies would benefit from the functionality that a more robust tool would provide.

In our discussions with MNIT, they noted that they had already begun the process of identifying and selecting a tool that will meet the agency's needs of managing enterprise-wide disaster recovery tasks. We encourage MNIT to continue this effort in its governance and oversight of disaster recovery for the state's systems and technical infrastructure.

RECOMMENDATIONS

- **MNIT should ensure that disaster recovery data is complete and accurate.**
- **MNIT should consider implementing an enterprise continuity management and planning tool.**

Information Technology Disaster Recovery Plans

We reviewed the information technology disaster recovery (IT DR) plans for four state systems. All four of these systems are defined as Priority 2 applications, which means an extended period of downtime—beyond one week—could have a significant impact on state government operations or the public.

As criteria for our audit, we utilized guidance published by the National Institute of Standards and Technology (NIST), which are considered best practices for IT DR planning and apply to all information systems.[14]

Medicaid Management Information System (MMIS)

The Department of Human Services (DHS) uses the Medicaid Management Information System (MMIS) to process healthcare claims and payments to service providers, and capitation payments to DHS-contracted managed care organizations. MMIS is the system of record for much of the agency's healthcare claims and related data. Without MMIS, the state would be unable to make payments to various care providers or produce required federal reporting data.

MMIS relies heavily on the MNIT Enterprise mainframe disaster recovery plan. This plan is supported centrally by MNIT's mainframe team and documents how to restore the state's mainframe system and application services supporting several agencies in the event of a disaster.

MNIT, in partnership with the Department of Human Services, is prepared to recover its mainframe and Medicaid Management Information System.

Our review of the mainframe and MMIS IT DR plan found that:

- MNIT had an IT DR plan in place—generally adhering to best practices—for its mainframe and MMIS.

[14] U.S. National Institute of Standards and Technology, Special Publication 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*, November 2010, provides specific instructions and recommendations for information technology system disaster recovery planning activities. U.S. National Institute of Standards and Technology, Special Publication 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, December 2020, section 3.6, pp. 115-130, describes disaster recovery controls and planning tasks that organizations should implement for information systems.

- The state mainframe and its dependent systems, such as MMIS, can be restored within an alternative data center in the event of a disaster.

- MNIT, with participation from DHS, performs annual tests of the mainframe and MMIS IT DR plan.

Minnesota Eligibility Technology System (METS)

The Minnesota Eligibility Technology System (METS) is an enrollment and eligibility system that supports the services of two state agencies: the Department of Human Services (DHS) and MNsure. METS determines Minnesotans' eligibility for Minnesota's insurance affordability programs—Medicaid, MinnesotaCare, and qualified health programs with advanced premium tax credits. It also interfaces with other systems, such as MMIS, to provide the necessary information required for payment or coverage. More than one million Minnesotans use METS to apply for and manage their benefits for the state's insurance affordability programs, while caseworkers throughout the state also rely on METS to assist those Minnesotans in processing changes to their accounts and coverage renewals. If METS were unavailable, Minnesotans would be unable to apply for any of Minnesota's insurance affordability programs through MNsure. Furthermore, caseworkers would have limited ability and access to assist healthcare applicants and enrollees.

MNIT, in partnership with the Department of Human Services and MNsure, is prepared to recover the Minnesota Eligibility Technology System.

Our review of the METS IT DR plan found that:

- MNIT had an IT DR plan in place—generally adhering to best practices—for METS.

- MNIT can restore METS in an alternative data center.

- MNIT, with participation from DHS and MNsure staff, performs annual testing of the METS IT DR plan.

Integrated Tax System (GenTax)

The Integrated Tax System supports a variety of services for the Minnesota Department of Revenue (DOR). The system is often referred to as GenTax, the name of the commercial, off-the-shelf tax administration software on which the system is built. If the system were unavailable, taxpayers' abilities to file and pay state taxes, the processing of tax filings, and the tracking or posting of deposits would be affected. The Department of Revenue's ability to register businesses and answer taxpayer questions would also be affected.

MNIT, in partnership with the Department of Revenue, is prepared to recover the GenTax System.

Our review of the GenTax IT DR plan found that:

- MNIT had an IT DR plan in place for the GenTax system, following best practices.
- MNIT can restore the GenTax system in an alternative data center.
- MNIT, with participation from DOR staff, performs multiple tests and exercises throughout the year of the GenTax IT DR plan.

Priority Level 2 Information Technology System

A fourth system, in which activities could be interrupted temporarily but must be recovered within a week, was also included in our audit scope. Due to weaknesses with the IT DR plan for this system, and in an effort to protect its security, we are not naming the system or providing additional details in this public report.

FINDING 2

MNIT and its partnering agency are not adequately prepared to restore one priority system within the desired timeframe.

While MNIT had an IT DR plan in place for this system, the plan was missing many essential details. For example, the plan did not contain a discussion of the impact of the system being unavailable. The plan was missing activation criteria—the procedures for invoking the plan—and what notification processes would occur. MNIT's plan was also missing critical detailed restoration procedures, often found within "runbooks."[15] Furthermore, the plan did not have detailed system validation testing procedures, outlining what steps would need to be completed to confirm the system was restored and functioning properly. Finally, the plan lacked an annual review, change logs, and testing.

MNIT had not validated that it can restore this fourth system in an alternative data center. This system's IT DR plan noted that the partnering agency needs the system restored and functional within four days of declaring a disaster. However, outside of the production, development, and test installations, MNIT did not have an alternative recovery site in place for this system. MNIT noted that they were working to enhance the system's recovery abilities within an alternative data center. However, this recovery strategy was not in place as of our audit. Based on the documented steps in the plan, it may take more than 12 days to fully recover the system from a disaster. Because MNIT and its partnering agency have not tested the system's plan, they can only estimate the system's restoration time. Exercises allow staff to execute their roles and responsibilities as they

[15] A runbook is a detailed "how-to" guide for completing a commonly repeated task or procedure within an organization's IT operations process.

would in an actual emergency situation, but in a simulated manner. An exercise or test of the IT DR plan would assist MNIT and its partnering agency in understanding how long restoration activities may actually take, in addition to ensuring that the plan is accurate and viable.

Finally, we noted that MNIT had not completed a risk assessment for this system. MNIT's Information Security Risk Management Standard requires that a risk assessment be performed on all "new and significantly changed systems."[16] Because this system has undergone recent updates, we believe that a risk assessment was necessary. Such an assessment will help MNIT and its partnering agency understand the system's current risks and gaps.

RECOMMENDATIONS

- **MNIT and its partnering agency should revise this system's disaster recovery plan and ensure that it meets best practices.**
- **MNIT and its partnering agency should exercise this system's disaster recovery plan at an alternative recovery site.**
- **MNIT and its partnering agency should perform a risk assessment on the system.**

[16] Minnesota Information Technology Services, *Information Security Risk Management Standard*, Control Number 2, version 1.4, approved March 10, 2020.

List of Recommendations

- MNIT should ensure that disaster recovery data is complete and accurate. (p. 15)
- MNIT should consider implementing an enterprise continuity management and planning tool. (p. 15)
- MNIT and its partnering agency should revise this system’s disaster recovery plan and ensure that it meets best practices. (p. 18)
- MNIT and its partnering agency should exercise this system’s disaster recovery plan at an alternative recovery site. (p. 18)
- MNIT and its partnering agency should perform a risk assessment on the system. (p. 18)

OLA

Appendix

Executive Orders Issued for Emergency Responsibilities

State of Minnesota Executive Order Number	Title	Date
70-58	Executive Order No. 58	May 20, 1970
73-57	Assigning Emergency Responsibilities to State Agencies	March 26, 1973
75-102	Assigning Emergency Responsibilities to State Agencies	April 7, 1975
77-157	Assigning Emergency Responsibilities to State Agencies and Repealing Executive Orders 102 and 102A	October 12, 1977
79-03	Assigning Emergency Responsibilities to State Agencies; Repealing Executive Order 77-157	February 26, 1979
81-03	Assigning Emergency Responsibilities to State Agencies; Repealing Executive Order 79-3	March 4, 1981
83-17	Assigning Emergency Responsibilities to State Agencies; Repealing Executive Order 81-3	March 15, 1983
85-09	Assigning Emergency Responsibilities to State Agencies; Repealing Executive Order 83-17 [and] Executive Order 83-10	March 1, 1985
88-2	Assigning Emergency Responsibilities to State Agencies; Repealing Executive Order 85-9	January 15, 1988
90-2	Assigning Emergency Responsibilities to State Agencies; Rescinding Executive Order 88-2	May 31, 1990
93-27	Assigning Emergency Responsibilities to State Agencies; Rescinding Executive Order 90-2	December 10, 1993
96-16	Assigning Emergency Responsibilities to State Agencies; Rescinding Executive Order 93-27	August 27, 1996
99-20	Assigning Emergency Responsibilities to State Agencies; Rescinding Executive Order 96-16	December 29, 1999
04-04	Assigning Emergency Responsibilities to State Agencies; Rescinding Executive Order 99-20	March 29, 2004
07-14	Assigning Emergency Responsibilities to State Agencies; Rescinding Executive Order 04-04	September 7, 2007
10-06	Assigning Emergency Responsibilities to State Agencies; Rescinding Executive Order 07-14	April 26, 2010
11-03	Assigning Emergency Responsibilities to State Agencies; Rescinding Executive Order 10-06	January 14, 2011
13-13	Assigning Emergency Responsibilities to State Agencies; Rescinding Executive Order 11-03	November 26, 2013
15-13	Assigning Emergency Responsibilities to State Agencies; Rescinding Executive Order 13-13	July 13, 2015
15-14	Directing Implementation of the Minnesota Continuity of Government Plan	July 13, 2015
19-22	Assigning Emergency Responsibilities to State Agencies; Rescinding Executive Order 15-13	April 4, 2019
19-23	Directing the Development and Maintenance of the Minnesota Continuity of Government Plan and Agency Continuity of Operations Plans; Rescinding Executive Order 15-14	April 4, 2019

OLA

MINNESOTA

September 26, 2022

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

Dear Ms. Randall,

Thank you for the opportunity to review and comment on your office's report on "Disaster Recovery Strategies for Critical IT Systems." Minnesota IT Services (MNIT) and Minnesota Management and Budget (MMB) appreciate the time and effort put forth by your office in the development of this report and the opportunities your office's work provides to highlight areas of potential risk and strengthen state agency processes and policies. MNIT and MMB are responding jointly to this report, as our agencies have shared responsibility in this space. MNIT has oversight over enterprise information technology and MMB has oversight over enterprise continuity of operations planning. As described in additional detail below, we have already taken significant steps responsive to each finding, standing up disaster recovery capabilities for the system identified in Finding 2 and acquiring a software tool that will replace the manual processes noted in Finding 1.

Recognizing the responsibility we have to ensure the continuity of information technology upon which so many state services and Minnesotans rely, Minnesota IT Services – working in partnership with our business partner state agencies – has made the development and maintenance of effective IT disaster recovery capabilities a critical focus for the State's executive branch, particularly considering the ever evolving and increasing rate of ransomware attacks targeting both private and public organizations. Over the past several years, through our centralized disaster recovery planning and oversight program, we have put specific focus on refreshing disaster recovery plans, verifying business partner agency recovery time and recovery point objectives, and exercising disaster recovery processes and procedures. We have also prioritized working with our business partner agencies and the Minnesota Legislature to ensure that sufficient resources are provided to support disaster recovery capabilities that align with the priorities and recovery timelines of agency priority services.

We appreciate the OLA's recognition that "MNIT has centralized policies and procedures to provide effective oversight and management of disaster recovery planning efforts" and that "in the event of a disaster, MNIT, and its partnering agencies are prepared to recover the Medicaid Management Information System (MMIS), the Minnesota Eligibility Technology System (METS), and the Integrated Tax System."

As it relates to Finding 2 and the fourth system in scope of this audit report, for which the report concludes that "MNIT and its partnering state agency are not adequately prepared to restore one priority system within the desired timeframe," we wish to make very clear that the report does not reflect the current state of disaster recovery capability for that system. As noted in the report, the audit period for this report concluded in November 2021, nearly 11 months ago. After unsuccessful attempts to secure funding via the legislative budgeting process, one-time dollars were identified to stand up disaster recovery capabilities for this system. However, the ability to maintain this capability moving forward is uncertain given current funding levels. We anticipate requests in future legislative sessions will likely be proposed to ensure this critical capability can remain in place.

As it relates to Finding 1, that "MNIT's manual disaster recovery tracking process lacks functionality and is prone to human error," we recognize and share the concern that manual processes increase the risk of human error. For that reason, MNIT has partnered with the Departments of Transportation, Corrections, and Education to identify a software tool to automate our continuity of operations and IT disaster recovery planning and move away from manual planning. We gathered input on over 100 software requirements from state agency partners, local government agencies, and other interested parties such as MNIT service delivery operations, procurement, and security functions. We acquired such a software tool in July 2022 and have been working since that time to implement the software, including developing standard planning templates, integrating data from other state systems, and training users. We have also discussed future options with the Continuity Policy Coordination Sub-Cabinet about having the software as an enterprise offering for all state agencies. We expect to roll out the software to these four initial agencies by the end of the second quarter of FY2023.

While ensuring disaster recovery capability is a major focus for MNIT, we feel it is important to note that sustaining and securing IT systems to prevent such disaster scenarios from occurring in the first place must be treated with similar urgency and focus. Minnesota state government services rely upon a host of IT systems across the executive branch that will require modernization in the near future to be fully supported. Moreover, some systems lack sufficient funding for current maintenance and operations activities, such as version upgrades and software vulnerability remediation, that require sustainable funding to properly manage risk. Ensuring appropriate disaster recovery capabilities requires the careful alignment of agency priority services with continuity of operations capabilities, recovery expectations, recovery capabilities, and the resources necessary to support these capabilities. The incremental levels of IT continuity capabilities that can be implemented in any organization correspond to incremental increases in costs. A similar need to balance cost and risk is present in system sustainability and security. It is the responsibility of state leaders in both the executive and legislative branches of state government to manage that risk and cost equation to appropriately safeguard against service delivery disruptions that could put public health and safety and the economic vitality of Minnesota at risk.

Again, we appreciate the work of OLA staff and leadership and the productive and professional working relationships that have been established between our agencies and your office over the course of this and other audits. We look forward to working with members of the Legislature and the Office of the Legislative Auditor moving forward to examine and address areas of risk as we work to transform and modernize agency operations through the application of technology tools and services.

Sincerely,

Commissioner Tarek Tomes
Minnesota IT Services

Commissioner Jim Schowalter
MMB

Financial Audit Staff

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

Audit Directors
Ryan Baker
Jordan Bjonfald
Kayla Borneman
Mark Mathison
Heather Rodriguez
Valentina Stone
Scott Tjomsland
Zach Yzermans

Audit Coordinators
Joe Sass

Senior Auditors
Tyler Billig
Bill Dumas
Scott Dunning
Daniel Hade
Shannon Hatch
Gabrielle Johnson
Lisa Makinen
Alec Mickelson
Crystal Nibbe
Duy (Eric) Nguyen
Erick Olsen
Sarah Olsen
Amanda Sayler
Emily Wiant

Staff Auditors
Ria Bawek
Nicholai Broekemeier
Sarah Bruder
Andrea Hess
Zachary Kempen
Zakeeyah Taddese
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 7-1-1 or 1-800-627-3529.

♻ Printed on Recycled Paper

OLA

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