OLA

OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

Financial Audit Division Report

State of Minnesota
Continuity of Operations Plans

March 7, 2008 **08-07**

Financial Audit Division

The Office of the Legislative Auditor (OLA) is a professional, nonpartisan office in the legislative branch of Minnesota state government. Its principal responsibility is to audit and evaluate the agencies and programs of state government (the State Auditor audits local governments).

OLA's Financial Audit Division annually audits the state's financial statements and, on a rotating schedule, audits agencies in the executive and judicial branches of state government, three metropolitan agencies, and several "semi-state" organizations. The division also investigates allegations that state resources have been used inappropriately.

The division has a staff of approximately forty auditors, most of whom are CPAs. The division conducts audits in accordance with standards established by the American Institute of Certified Public Accountants and the Comptroller General of the United States.

Consistent with OLA's mission, the Financial Audit Division works to:

- Promote Accountability,
- Strengthen Legislative Oversight, and
- Support Good Financial Management.

Through its Program Evaluation Division, OLA conducts several evaluations each year.

OLA is under the direction of the Legislative Auditor, who is appointed for a six-year term by the Legislative Audit Commission (LAC). The LAC is a bipartisan commission of representatives and senators. It annually selects topics for the Program Evaluation Division, but is generally not involved in scheduling financial audits.

All findings, conclusions, and recommendations in reports issued by the Office of the Legislative Auditor are solely the responsibility of the office and may not reflect the views of the LAC, its individual members, or other members of the Minnesota Legislature.

To obtain a copy of this document in an accessible format (electronic ASCII text, Braille, large print, or audio) please call 651-296-1235. People with hearing or speech disabilities may call us through Minnesota Relay by dialing 7-1-1 or 1-800-627-3529.

All OLA reports are available at our web site: http://www.auditor.leg.state.mn.us

If you have comments about our work, or you want to suggest an audit, investigation, or evaluation, please contact us at 651-296-4708 or by e-mail at auditor@state.mn.us

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

Financial Audit Division Report

State of Minnesota

Continuity of Operations Plans

March 7, 2008 **08-07**

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

This page intentionally left blank.

OLA

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

Representative Rick Hansen, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Mr. Gopal Khanna, State Chief Information Officer
Office of Enterprise Technology

Mr. Christopher Buse, Chief Information Security Officer
Office of Enterprise Technology

We have conducted an audit of the state's continuity of operations plans. The scope of our audit focused on processes that help to ensure, in the event of a disruption, state government's mission critical services and operations recover in a timely manner. The Report Summary highlights our overall conclusion. Our specific audit objective and conclusion are contained in Chapter 2 of this report. This audit contains two findings related to internal control weaknesses.

We would like to thank the staff from the Office of Enterprise Technology, and all other agencies that participated, for their cooperation during this audit.

/s/ James R. Nobles

James R. Nobles
Legislative Auditor

/s/ Cecile M. Ferkul

Cecile M. Ferkul, CPA, CISA
Deputy Legislative Auditor

Room 140 Centennial Building, 658 Cedar Street, St. Paul, Minnesota 55155-1603 • Tel: 651/296-4708 • Fax: 651/296-4712
E-mail: auditor@state.mn.us • TDD Relay: 651/297-5353 • Website: www.auditor.leg.state.mn.us

State of Minnesota
Continuity of Operations Plans

Table of Contents

Audit Participation

The following members of the Office of the Legislative Auditor prepared this report:

Cecile Ferkul, CPA, CISA	Deputy Legislative Auditor
Eric Wion, CPA, CISA, CISSP	Audit Manager
Carolyn Engstrom, CISA	Auditor-in-Charge
Bill Betthauser	Auditor

Exit Conference

We discussed the findings and recommendations with the following representatives of the Office of Enterprise Technology at the exit conference held on February 26, 2008:

Gopal Khanna	State Chief Information Officer
Chris Buse	State Chief Information Security Officer
Mark Mathison	Compliance Manager
Siri Johnson	BCM Systems Architect
Deb Stafford	Investigative and Corrective Controls Supervisor

State of Minnesota
Continuity of Operations Plans

Report Summary

Conclusion:

The State of Minnesota does not have adequate continuity of operations plans to ensure the timely recovery of critical services and operations in the event of a disruption.

Findings:

- Most large state agencies have a continuity of operations plan, but many of the plans are out-of-date, lack adequate recovery strategies, and have not been adequately tested. (Finding 1, page 7)
- The Office of Enterprise Technology has not addressed all of the components of its continuity of operations framework. (Finding 2, page 9)

Audit Scope:

We assessed business continuity controls as of November 2007.

Background:

A continuity of operations plan is a documented plan used by an organization to respond, recover, resume, and restore people, business processes, and technology from a disruption. A disruption can result from many events, including disasters like tornadoes, floods, fires, or widespread illnesses. Other events like computer viruses, computer failures, terrorism, or chemical spills can also cause disruptions in an organization's operations. In addition to continuing to provide critical services during major business interruptions, government has the added responsibility of continuing governance itself.

This page intentionally left blank.

Chapter 1. Introduction

Sometimes disaster happens, and the state needs to respond to ensure the public safety of its citizens. Recent events, such as the I-35W bridge collapse and the flooding in portions of Minnesota, have demonstrated that the state and other government agencies can respond to these types of events.

However, what happens when the disaster hits state government and disrupts its ability to provide critical public services? What if important state buildings were damaged? What if the state's computer systems were not available? What if the state's workforce was unable to report to work? In the event of a disaster, how would the state continue to govern? These questions are the focus of continuity of operations planning.

Many events could disrupt the state's ability to provide important services, such as natural disasters like tornadoes, floods, or fires; widespread illnesses; computer viruses or computer failures; or terrorism. Should an event happen that results in the disruption of government operations, the state would still need to make pension payments, deposit tax revenues, provide aid to schools, local governments, and needy families, and many other important services.

Having up-to-date, documented, tested continuity of operations plans in place increases the likelihood that the state can recover from a disruption and continue to provide its critical services. When a disruption occurs, a continuity of operations plan puts into action predetermined steps to restore people, processes, and technology needed to support operations.

Audit Approach

We conducted this audit in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. To assess the state's continuity of operations planning, we used criteria contained in the *Control Objectives for Information and Related Technology (COBIT),* the Business Continuity Institute's *Good Practice Guidelines,* and the Office of Enterprise Technology's *Enterprise Security Policy on Continuity of Operations* (07-01) and its supporting standard.[1]

[1] COBIT, published by the IT Governance Institute, is an IT governance framework providing organizations with a set of generally accepted measures, indicators, processes, and best practices to assist them in developing appropriate IT governance and control in an organization. The Good Practice Guidelines, published by the Business Continuity Institute, were developed by a committee of continuity professionals and designed to capture best practices covering the whole continuity management lifecycle.

This page intentionally left blank.

Chapter 2. Continuity of Operations Planning

Chapter Conclusion

The State of Minnesota does not have adequate continuity of operations plans to ensure the timely recovery of critical services and operations in the event of a disruption.

By failing to adequately plan for disruptions, some state agencies may be unable to conduct business for prolonged timeframes. This may prevent citizens from receiving critical government services and have a significant and unanticipated financial cost to government. In addition, government's inability to manage a disruption effectively may deteriorate citizens' perceptions of government.

Until recently, the State of Minnesota had a decentralized model for continuity planning. Each state agency was expected to develop its own continuity of operations plan with minimal direction or oversight. There was little, if any, government-wide continuity planning and strategy development. As a result, continuity planning and controls varied greatly among state agencies.

In 2005, the Legislature created the Office of Enterprise Technology (OET). OET began to coordinate the state's efforts to manage and secure its technology-related investments and coordinate the state's continuity of operations planning. In late 2006, OET formed a committee that included participants from several state agencies to draft a policy and standard governing the development and maintenance of a continuity of operations plan. After a lengthy period of review and discussion, the state's first continuity of operations policy and standard became effective January 2008. The policy requires compliance by executive branch agencies, offices, councils, boards, and commissions by July 2011.

The OET policy and standard defined the roles and responsibilities of both OET and other state agencies. OET's responsibilities include:

1. Establishing policies and procedures for managing the business continuity program for the State of Minnesota;
2. Managing recovery strategy funding;
3. Providing and maintaining templates that agencies can use to develop their plan;
4. Providing and maintaining an enterprise tool, or computer system, that agencies must use to develop their plan;
5. Providing planners to assist agencies in developing their plan; and
6. Reviewing each agency's plan to ensure it addresses critical steps.

State of Minnesota
Continuity of Operations Plans

The policy and standard require state agencies to develop a continuity of operations plan and maintain it on an ongoing basis. Table 2-1 identifies the steps required by OET's standard.

Table 2-1
Steps Required to Develop a Continuity of Operations Plan

Step	Purpose
Risk Assessment	Identifies potential events that could adversely affect the agency, the damage such events might cause, and the controls needed to prevent or minimize the impact. Agencies must perform a risk assessment after any major change to agency operations or at least every four years.
Business Impact Analysis	• Identifies all time-sensitive services, processes, and functions, resources and infrastructure, and assesses the impact of a disruption. • Determines how long critical functions, resources, and infrastructure can be unavailable before significant consequences result. • Considers how processes interface with other government agencies, vendors, and service providers. This analysis must include adequate representation from all business units and be validated and approved by agency management. State agencies must perform an analysis after any major change to the agency or at least every four years.
Recovery Strategy	Identifies the specific steps needed to recover critical operations and services in a predetermined amount of time. Agencies must participate in recovery solutions centrally managed by OET.
Plan Documentation	Ensures the agency can respond to an incident, recover and resume the critical processes, and return to normal operations in a structured, orderly, and timely manner. An agency must store and maintain its plan documentation in the state's continuity planning software centrally managed by OET.
Periodic Plan Exercises and Maintenance	Verifies the plan is current and will work. Agencies must test and maintain their plan at least annually and report the results to OET.
Awareness and Training Program	Ensures all employees understand their roles and responsibilities in the event of a disruption.

Source: Office of Enterprise Technology *Enterprise Security Standard on Continuity of Operations 2007 – 01*.

State of Minnesota
Continuity of Operations Plans

Our audit objective was to answer the following question:

- Does the State of Minnesota have adequate continuity of operations plans to ensure the timely recovery of critical services and operations in the event of a disruption?

To answer this question, we interviewed key personnel at OET and various state agencies, surveyed 20 executive branch agencies, and reviewed relevant documentation.

Current Findings and Recommendations

1. Most large state agencies have a continuity of operations plan, but many plans are out-of-date, lack adequate recovery strategies, and have not been adequately tested.

We surveyed 20 executive branch agencies and questioned them about their continuity of operations plans. Table 2-2 lists agencies surveyed.

Table 2-2
List of Executive Branch Agencies Surveyed

Administration	Enterprise Technology	Natural Resources
Agriculture	Finance	Pollution Control
Commerce	Health	Public Safety
Corrections	Human Rights	Revenue
Education	Human Services	Transportation
Employee Relations	Labor and Industry	Veterans Affairs
Employment and Economic Development	Military Affairs	

Based on their responses, none of these agencies was well prepared to resume operations after a disruption. Plans had the following significant deficiencies:

- Plans did not exist or were out-of-date
- Plans lacked adequate recovery strategies
- Plans were not adequately tested

Information obtained from agency surveys included security-related information that the Minnesota Data Practices Act classifies as nonpublic.[2] To protect state resources and comply with the Minnesota Data Practices Act, we withheld specific security-related details from this publicly released report. We communicated all pertinent details to the management of the Office of Enterprise Technology in a separate, nonpublic document.

[2] The information is classified by *Minnesota Statutes* 2007, 13.37(a). The classification was confirmed by the Commissioner of Administration in an opinion dated November 22, 2004.

Table 2-3 summarizes the results of the business continuity planning survey.

Table 2-3
Continuity of Operations Survey
Summary of Results

Step	Results
Risk Assessments	16 agencies completed a risk assessment; however, 12 had not done so in over four years. 4 agencies never completed a risk assessment.
Business Impact Analysis	16 agencies completed an impact analysis; however, 12 had not done so in over four years. 4 agencies had not completed an impact analysis.
Recovery Strategy – Key Personnel	11 agencies identified a location to which their critical staff should relocate in the event of a disruption. 9 agencies had not developed a plan at all or had only assumed they would relocate critical staff, but had not identified a suitable location.
Recovery Strategy – IT Facilities	12 agencies had plans to relocate some of its most critical IT facilities, including computer equipment, to an alternate facility. 8 agencies had not developed a plan at all or had only assumed they would acquire both space and computer equipment after a disruption occurs.
Plan Documentation	11 agencies had documented their plans in the state's continuity planning software. 6 agencies had documented their plans outside of the state's continuity planning software. 3 agencies had not documented a plan.
Periodic Plan Exercises and Maintenance	8 agencies tested portions of their plan annually, while 2 agencies had only tested their plan once or on an ad hoc basis. 10 agencies had never tested.
Awareness and Training Program	5 agencies had a continuity awareness program and 15 agencies did not have such a program.

Source: Prepared by the Office of the Legislative Auditor.

Most agencies identified a lack of resources and priority or urgency as their top barriers to developing and maintaining a continuity of operations plan. Seven agencies stated they had not budgeted funds for continuity. Twelve said they had allocated less than one person's time to support their agency's continuity efforts. Effective continuity planning requires the ongoing allocation of funds and staff resources.

Failure to adequately plan for and recover from a disruption could have a devastating impact. Each agency surveyed is responsible for processes that are critical to the ongoing operation of government or the well being and safety of the state's citizens. For example, the state collects over $15 billion in individual, corporate, sales, and other taxes each year that fund a significant portion of the state's activities. The state provides essential aid to thousands of citizens, including over $630 million to over 170,000 unemployed people each year. Each year, the state pays over $5 billion to medical providers to help pay for medical care for over 450,000 low-income seniors, children and parents, and people with disabilities. These are just a few of the countless important functions state agencies provide. Their failure to develop up-to-date and

tested continuity of operations plans may jeopardize their ability to fulfill their missions in the event of a significant disruption.

Recommendation

- *Agencies should develop continuity of operations plans in accordance with OET's Continuity of Operations Policy and Standard.*

2. OET has not addressed all of the components of its continuity of operations framework.

Although OET has made a good start in building a continuity of operations framework,[3] it has not fully addressed some plan components.

As discussed in Finding 1, a significant gap exists between state agencies current preparedness and being well prepared by complying with the new policy and standard. OET has not yet established a tactical plan to identify the steps, resources, and timelines needed to achieve continuity objectives and agency compliance with the continuity of operations policy.

Recognizing the importance of having a consistent approach to continuity planning and a centralized repository for all executive branch agency plans, the new policy requires OET to maintain templates and a continuity planning software that agencies must use to develop and document plans. In some cases, OET has not developed templates to gather important information from agencies and upload it into the software. In other cases, OET has templates, but the office has not developed a process to upload the data into the software. The software may require additional customization to accommodate new or modified templates. After template and software changes, OET will need to document a user manual to instruct people on how to use the templates and software.

Finally, the state does not currently have a government-wide funding model to implement its new continuity of operations policy and standard. OET needs to take the lead to determine how much funding is needed and where the funds will come from.

[3] OET has developed a policy and standard for the executive branch's continuity of operations plans, required that agencies use a centralized and standardized computer application to document their plans, and dedicated a small staff with specialized continuity training and skills to assist agencies in plan development.

Recommendations

- *OET should establish a tactical plan to identify the steps, resources, and timelines needed to achieve continuity objectives and agency compliance with the continuity of operations policy.*

- *OET should develop new and update existing continuity planning templates and processes to ensure agencies gather the correct information and it is uploaded into the continuity planning software. In addition, OET should document a user manual to instruct people on how to use the templates and software.*

- *OET should work with executive branch leaders and the legislature to develop a funding model for the state's continuity of operations plans.*

March 3, 2008

James R. Nobles, Legislative Auditor
Office of the Legislative Auditor
658 Cedar Street 140
Centennial Office Building
St. Paul, MN 55 155-4708

Dear Mr. Nobles:

Thank you for the opportunity to discuss your audit findings for the Statewide Business Continuity Controls Audit. We place a high priority on business continuity controls and are committed to helping the state solve the problems that we now face. The report's conclusion is the same message that we have conveyed at legislative hearings, security briefings, to state CIOs, the Governor's cabinet, and at both Enterprise Security Summits held for state leadership: the state must have actionable and tested continuity of operations in place. We appreciate your endorsement of the direction we are heading and agree that there is much to be done.

Finding 1: Most large state agencies have a continuity of operations plan, but many plans are outdated, lack adequate recovery strategies, and have not been adequately tested.

Recommendation: Agencies should develop continuity of operations plans in accordance with OET's Continuity of Operations Policy and Standard.

Office of Enterprise Technology Response:

We agree with the finding and recommendation and made similar conclusions ourselves a year ago shortly after establishing an enterprise security program and hiring the state's first Chief Information Security Officer. At that time, we began working on a policy and standard for continuity of operations, which went into effect December 31, 2007, and is referenced in your recommendation.

Getting all state agencies to agree on a policy and standard was a major accomplishment. We now plan to work with state agencies to bring them into compliance with these documents that outline the collective vision of what needs to be done to bridge the gap from where we are today to where we need to be.

The policy and standard include a three-year compliance window that closes June 30, 2011. The length of this window reflects the magnitude of the work that must be done to rectify the current problems. Significant investments at both the agency and enterprise level will be needed to meet the requirements. We will work with our security colleagues and leadership to identify and secure the resources to stay on target.

Finding 2: OET has not addressed all the components of its continuity of operations framework.

Recommendation 1: OET should establish a tactical plan to identify the steps, resources, and timelines needed to achieve continuity objectives and agency compliance with the continuity of operations policy.

Recommendation 2. OET should develop new and update existing continuity planning templates and processes to ensure agencies gather the correct information and it's uploaded into the continuity planning software. In addition, OET should document a user manual to instruct people on how to use the templates and software.

Recommendation 3: OET should work with executive branch leaders and policy makers to develop a funding model for the state's continuity of operations plans.

Office of Enterprise Technology Response:

We agree with the finding and recommendations.

We will continue to work with state agencies to develop a tactical plan. A working group, composed of continuity planners from various agencies, has been formed to develop the enterprise continuity planning process. The group meets regularly and has begun working on the various components documented in the continuity of operations standard.

We have improved access to two planners to help those agencies that need help with their continuity planning, and we have funded a state-of-the-art COOP planning tool to assist agency planners.

We also are committed to developing robust processes to make continuity planning easier and more cost-effective. Part of this effort will include the creation of a manual to help agencies use the new electronic templates and software.

We agree with the report that, although it is important to develop written plans, it is arguably more important to test those plans to make sure that they really will work in the event of a crisis. Commonly referred to as "recovery strategies," this area is one where the audit was extremely critical of our current capabilities. It also is the most costly aspect of the problem. We will work with government leaders to develop a viable funding model, as recommended by the audit.

Chief Information Security Officer Chris Buse is responsible for addressing the findings in this report for the Office of Enterprise Technology and for managing compliance among state agencies.

Before closing, I would like to thank the members of the audit team for their professionalism and understanding of the significant challenge we, as a state, face in keeping government safe and in operation at all times, under all circumstances.

Sincerely,

Gopal Khanna
State CIO