City of Milwaukee

Office of the Comptroller

W. Martin Morics, C.P.A.
Comptroller

Michael J. Daun
Deputy Comptroller

John M. Egan, C.P.A.
Special Deputy Comptroller

Craig D. Kammholz
Special Deputy Comptroller

August 19, 2010

To the Honorable
the Common Council
City of Milwaukee

Dear Council Members:

Enclosed is a report to the City's Chief Information Officer on our Audit of IT Disaster Recovery Plans for three selected departments.

The Audit disclosed that the Information and Technology Management Division was the only department with a formal written plan. The audit makes three recommendations, including the development of disaster recovery plans for all city divisions hosting major City information systems. The Chief Information Officer's response is also enclosed.

Appreciation is expressed to ITMD, the Department of Public Works and Office of the City Treasurer for the full cooperation extended to the auditors.

Sincerely,

Michael J. Daun

W. MARTIN MORICS
Comptroller

CC: Nancy A. Olson, CIO
Jeffrey J. Mantes, DPW Commissioner

City of Milwaukee

Office of the Comptroller

W. Martin Morics, C.P.A.
Comptroller

Michael J. Daun
Deputy Comptroller

John M. Egan, C.P.A.
Special Deputy Comptroller

Craig D. Kammholz
Special Deputy Comptroller

July 12, 2010

Nancy Olson
Chief Information Officer
Department of Administration
809 North Broadway, Suite 400
Milwaukee, WI 53202

Subject: IT Disaster Recovery Audit

Dear Ms. Olson:

The IT Disaster Recovery Plans of Information Technology Management Division, the Department of Public Works and The Office of the City Treasurer were selected for audit based upon KPMG's suggested Disaster Recovery Audit as part of the IT internal audit plan. ITMD and DPW were selected as they control a large portion of the City's IT as well as the Treasurer's office which has unique systems. ITMD was the only department that had a formal written Disaster Recovery Plan. This plan contained most of the key components for a quality Disaster Recovery Plan.

It is the City of Milwaukee's policy that all City departments are to have a Disaster Recovery Plan, however no further guidance as to what should be included and covered in the plan is specified. We recommend that the CIO coordinate an effort to develop a plan for implementation throughout all City departments including guidance on how to develop and implement a Disaster Recovery Plan and what should be covered in the plan. Please see the attached report for further information.

If you have any questions or concerns, please contact Isaak Lerner at 286-2382.

Sincerely,

Michael J. Daun

W. MARTIN MORICS
Comptroller

An IT Disaster Recovery Plan (DRP) is the process, policies and procedures used in preparing for the recovery of technology critical to an organization after a natural or human-induced disaster. Information technology has become increasingly important to the City's ability to function in recent years so ensuring that the City's data and IT infrastructure are properly protected in the event of a disruption is a necessity. IT systems are vulnerable to many disruptions ranging from mild (short-term power outage) to severe (total equipment destruction, fire). Although it is impossible to eliminate all risks, many can be minimized through proper risk management planning. A Disaster Recovery Plan is necessary to mitigate the risk of system unavailability by focusing on recovery solutions.

The City of Milwaukee would not be totally prepared in the event of a disaster. Three City of Milwaukee departments, ITMD, DPW and the Office of the City Treasurer were interviewed. ITMD was the only department with a documented DRP. According to The City of Milwaukee's Information and Security Policies and Standards document, all City departments are to have a Disaster Recovery Plan, however no further guidance as to what should be included and covered in the plan is specified.

The Treasurer's Office and the DPW do not have formal written plans, however they do have an inventory of hardware and software and the Treasurer's Office has backups that are stored off-site. ITMD's DRP includes all of the key components, with the exception of testing the plan annually.

Recommendation # 1: ITMD should test the Disaster Recovery Plan annually

ITMD has developed an adequate disaster recovery plan through its collaboration with Homeland Security. While the plan contains all the critical sections of a complete DRP it has not been tested. The most comprehensive test of the DRP would involve a simulated outage of key systems and their restoration using the steps outlined in the plan. If both computing and human capital resources are not available for a simulated outage test it is acceptable to perform a "Table Top" disaster recovery test once a year. During a table top test all key participants gather in a room and walk through the plan step by step. Table top exercises can effectively demonstrate whether team members know their duties in an emergency. Documentation errors, missing information and inconsistencies across the disaster recovery plan can be identified.

Recommendation #2: All departments should have a documented Disaster Recovery Plan

Since ITMD has shown its ability to create a quality DRP and has the IT knowledge that other departments may be lacking, we recommend that the CIO coordinate an effort to develop a plan for implementation throughout all City departments including guidance on how to prepare and implement a Disaster Recovery Plans and what should be covered in the plan. These details should be present in the IS Security Policy regarding DRP.

All City departments should develop a disaster recovery plan that is based on a complete business impact analysis which will help in identifying risk, critical information systems and the costs associated with various risks. A departmental business impact analysis will serve as the foundation for an efficient and risk based approach to defining the recovery requirements and priority of critical business applications in the event of disaster.
The following components should be addressed in each department's DRP;

- A formal written plan exists
- The plan has been based off of a Business Impact Analysis
- The plan is updated at least annually
- All critical systems are covered
- Inventory of all hardware and software is kept
- Systems are prioritized for recovery
- There are procedures for activation
- Someone is responsible for administration and coordination of the plan
- There is a disaster recovery implementation team that has been trained on the plan
- The plan is stored off-site

- Backups are kept off-site
- The plan has been tested

Recommendation # 3: DPW data backup media should be stored off-site

In the interview with DPW, it was discovered that their data backups are stored on-site. Sound procedures for backup and restoration are vital for the reconstruction of systems after a disruptive event. Data should be backed up regularly and stored at a secure, offsite facility such as Iron Mountain or another secure facility at least five miles from the DPW network operations center.

City of Milwaukee

Department of Administration
Information and Technology
Management Division

Tom Barrett
Mayor

Sharon D. Robinson
Administration Director

Nancy A. Olson
Chief Information Officer

August 9, 2010

W. Martin Morics
Comptroller
200 E Wells St, Room 404
Milwaukee, WI 53202

Subject: Management Response to IT Disaster Recovery Audit Findings

Dear Mr. Morics:

In your letter of July 12, 2010, you outlined the results of the internal IT Disaster Recovery audit conducted by your office. In that letter you provided three recommendations.

I offer the following proposal regarding these recommendations:

1. ITMD should test the Disaster Recovery Plan annually

Because ITMD does not have the computing and human resources to simulate an outage test we will perform a "Table Top" disaster recovery test in 2010. Since ITMD has no experience with this type of disaster recovery exercise, I would appreciate the experience of the IT auditor, Isaak Lerner. With Mr. Lerner's help, I believe that this will be a valuable exercise.

2. All departments should have a documented Disaster Recovery Plan

Starting in the fall of 2010, ITMD will conduct Disaster Recovery planning workshops and invite IT staff in other City departments to attend. These workshops will outline the elements of a disaster recovery plan and provide participants with the information needed to create a comprehensive departmental plan.

3. Department of Public Works data backup media should be stored off-site

ITMD currently uses a service from C.H. Coakley & Co. which picks up tapes weekly and rotates data backups offsite at a secure facility. DPW could include tapes in the pickup and delivery cycle at a significantly lower rate by sharing this service. ITMD recommends that DPW explore this option.

If you have questions, comments, or concerns please contact me at extension 8710. Thank you for your efforts at improving the safety and security of IT services throughout the City.

Sincerely,

Nancy A. Olson

Nancy A. Olson
Chief Information Officer
Information and Technology Management Division