

Martin Matson
Comptroller

John M. Egan, CPA
Deputy Comptroller



Glenn Steinbrecher, CPA
Special Deputy Comptroller

Toni Biscobing
Special Deputy Comptroller

Office of the Comptroller

June 5, 2013

To the Honorable
The Common Council
City of Milwaukee

Dear Council Members:

As a component of the 2013 audit work plan, the datacenter audit was performed the first quarter of 2013. Datacenter controls are an important and tangible part of ensuring that the City's computer systems are available and that City services connected to computing resources are not impaired. A datacenter must therefore maintain high standards for ensuring the security, integrity and functionality of its hosted computer environment.

A similar audit was conducted by the Audit Division in 2010 that resulted in several recommendations to improve datacenter security and sustainability. This audit also examined the implementation of the recommendations made in the 2010 audit at various datacenters.

The datacenter audit was conducted in February and March of 2013 and involved onsite visits of City operated data centers (secure rooms that contain server equipment on which City systems are housed). The objective of this audit is to verify that the current physical and environmental controls in place at City datacenters are appropriate and adhere to Information Systems (IS) security best practices.

The audit included physical tours of eight data centers throughout the City's departments and divisions including; Milwaukee Water Works, Department of Public Works, Police Department, Fire Department, Department of City Development, Library, Information Technology Management Division, and Municipal Court. Some datacenters and all networking/switch closets were not included in the scope for this audit. The Audit Division believes that the evidence obtained provides a reasonable basis for the audit findings and conclusions based on the audit objectives.

All datacenters were evaluated on the criteria of Data Center Physical and Environmental Control Standards published by the Information Systems Auditing and Control Association. The physical and environmental control areas were evaluated through physical tours and the examination of datacenter access listings and maintenance documentation. Controls evaluated during the datacenter audit were:

- Flood Prevention
- Fire Prevention
- Environmental Controls
- Access Controls
- Continuity Controls

The flood prevention controls evaluated included the presence of raised floors, drains, and leak detection systems. The fire prevention controls evaluated included the presence of smoke detectors, fire extinguishers, and fire suppression systems. The environmental controls evaluated included the presence of dedicated air conditioning, temperature/humidity controls, environmental alerts, secondary battery backup devices, proper cable management, and restricted physical access to the room. The other controls evaluated included the regular backup of data, datacenter capacity, and transportation of backup data to an alternate site.

The Audit Division's overall conclusion is that the City's various datacenters are in good operational standing and the physical, environmental and operating controls related to the datacenters are operating effectively with some exceptions.

The exceptions that were identified and the corresponding recommendations for improvement have been communicated to the appropriate City personnel. These exceptions are:

1. Three datacenters currently allow excessive privileged physical access.

Recommendation: Management should periodically review key card access listings and remove users or vendors who have no current business need to have access to the datacenter.

2. Two datacenters do not currently have fire extinguishers located within the room.

Recommendation: At least one ABC rated fire extinguisher should be clearly accessible inside the datacenter. The fire extinguishers should be serviced once a year.

3. One datacenter does not regularly take backups to an alternate site. This issue was noted in 2010 audit.

Recommendation: When data is backed up on physical media like tapes, CDs or DVDs, it should be taken to an alternate secure site at least once a week.

4. One datacenter experienced temporary elevated temperatures that can damage machines. The same issue was noted in 2010.

Recommendation: If a dedicated air conditioning unit is not providing adequate temperature control for several consecutive days then a secondary cooling unit should be installed in the datacenter.

Detailed findings and recommendations were sent to all datacenter IS managers and a written management response has been requested on the status of the individual recommendations. Management is currently finalizing their responses and mitigation plans.

Appreciation is expressed for the cooperation extended to the auditors by the staff of all City departments that were involved in the audit.

Sincerely,



Aycha Sirvanci, CPA
Audit Manager

CC: All division heads of departments audited
Nancy Olson, Chief Information Officer

AS:il