Audit of
ITMD Data Center Controls

MARTIN MATSON
City Comptroller

ADAM FIGON
Audit Manager

City of Milwaukee, Wisconsin

June 2018

Table of Contents

Martin Matson
Comptroller

Aycha Sirvanci, CPA, CIA
Deputy Comptroller

Toni Biscobing
Special Deputy Comptroller

Rocklan Wruck, CPA
Special Deputy Comptroller

Office of the Comptroller

June 13, 2018

Honorable Tom Barrett, Mayor
The Members of the Common Council
City of Milwaukee
Milwaukee, WI 53202

Dear Mayor and Council Members:

The attached report summarizes the results of the audit of the Information and Technology Management Division's (ITMD) Data Center controls. The scope of the audit included the ITMD Data Center's physical, environmental, and back-up control activities and included the alternate data processing site. The audit excluded the IT processes performed by departments that have not been administratively centralized within the ITMD. The audit scope does not include the Police and Fire Departments, Water Works, Municipal Court, Health Department, or Library. The time period covered includes the current state of operations and one complete data back-up cycle.

The primary focus of the audit was to evaluate whether the internal controls in place over the Data Center are adequately designed and operating effectively. The audit objectives were as follows:

1. Assess whether the data center physical and IT environmental controls are compliant with department policy, best practice criteria and standards outlined by ISACA, and

2. Assess whether the data center controls over data back-up, offsite storage and system restoration procedures are performed in accordance with department policy, best practice criteria and standards outlined by ISACA.

Overall, the audit concluded that the controls in place over physical, IT environmental, data-back up and offsite storage procedures are adequately designed and operating effectively. However, gaps exist in the operational effectiveness of system restoration and data center access controls. This report identifies three recommendations to address these issues.

Audit findings are discussed in the Audit Conclusions and Recommendations section of this report, and are followed by management's response.

City Hall, Room 404, 200 E. Wells Street, Milwaukee, WI 53202 • Phone (414) 286-3321 • Fax (414) 286-3281
www.milwaukee.gov/comptroller

Martin Matson
Comptroller

Aycha Sirvanci, CPA, CIA
Deputy Comptroller

Toni Biscobing
Special Deputy Comptroller

Rocklan Wruck, CPA
Special Deputy Comptroller

Office of the Comptroller

Honorable Tom Barrett, Mayor
The Members of the Common Council
Audit of the ITMD Data Center controls

Appreciation is expressed for the cooperation given to the auditors by the personnel of the ITMD and the Department of Public Works (DPW) Infrastructure Services Division.

Sincerely,

Adam Figon, MBA, CRMA
Audit Manager

ACF:bd

City Hall, Room 404, 200 E. Wells Street, Milwaukee, WI 53202 • Phone (414) 286-3321 • Fax (414) 286-3281
www.milwaukee.gov/comptroller

I. Audit Scope and Objectives

The scope of the audit encompassed the Information and Technology Management Division (ITMD) Data Center's physical, environmental and back-up control activities and included the alternate data processing site. The time period covered includes the current state of operations and one complete data back-up cycle.

The audit excluded the IT processes performed by departments that have not been administratively centralized within the ITMD. The audit scope does not include the Police and Fire Departments, Water Works, Municipal Court, Health Department, or Library.

Audit activities consisted of process walkthroughs, observations, review of policies and procedures and detailed testing of controls. During the performance of these audit activities, the data center's controls were evaluated using the IT environmental and back-up control standards published by the Information Systems Auditing and Control Association (ISACA). The data center was also evaluated based on adherence to City policy, procedure and best practice criteria.

Objectives

The objectives of the audit were as follows:

1. Assess whether the data center physical and IT environmental controls are compliant with department policy, best practice criteria and standards outlined by ISACA; and

2. Assess whether the data center controls over data back-up, offsite storage and system restoration procedures are performed in accordance with department policy, best practice criteria and standards outlined by ISACA.

The audit was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objectives. Internal Audit believes that the evidence obtained provides a reasonable basis for the audit's findings and conclusions based on the audit objectives.

Methodology

Audit methodology included developing an understanding of the processes and controls over the ITMD Data Center. To establish appropriate evaluation criteria for this audit, controls and procedures specific to the ITMD Data Center were compared to a best practice based controls testing program. This program was developed by using the Federal Information Systems Controls Audit Manual (FISCAM). FISCAM presents a methodology for performing information system control audits of federal and other governmental entities in accordance with professional standards (as presented in the *Generally Accepted Government Auditing Standards*, known as the "Yellow Book"). The audit program and procedures also included elements from best practice criteria COBIT/ISACA, COSO, and NIST 800-14 and 800-53 (Revision 4).[1] These standards were relevant during audit testing, finding identification, and recommendation development.

The audit procedures developed to evaluate the processes and controls to meet the audit objectives included process walk-throughs, inspection of relevant control documentation, and the testing of controls as follows:

- Review of internal policies, procedures, and guidelines;
- Review of physical access controls to the ITMD, ITMD Data Center, and Back-up Data Center facilities via employee key card access, based on the principle of least privilege;
- Assessment of environmental controls to protect against the risk of damage from fire, water, temperature irregularities and humidity, and unauthorized persons;
- Assessment of data back-up, offsite storage and system restoration procedures; and
- Evaluation of the business continuity plans to recover from a service outage.

II. Organization and Fiscal Impact

ITMD Mission

The ITMD provides IT-related services to City departments. These services include enterprise systems support, desktop support, networks and phones, major deployments of Citywide and

[1] - Control Objectives for Information and Related Technology (COBIT), created and managed by the Information Systems Audit and Control Association (ISACA);
- Committee of Sponsoring Organizations of the Treadway Commission -2013 (COSO);
- National Institute of Standards and Technology (NIST).

departmental IT systems, and server maintenance. In addition to staff and resource consolidation, ITMD works closely with City departments to replace outdated IT systems with more efficient systems that are simpler to maintain and provide enhanced functionality and greater coordination among the departments. The ITMD's mission is to lead the City in using and sharing information in ways that will provide the maximum efficiency and greatest benefit to Milwaukee citizens, businesses, and City government. Figure 1 below illustrates select ITMD relationships with other City departments.

Figure 1

The 2018 capital budget provides $1.6 million for ITMD projects. New projects planned for 2018 include a PeopleSoft upgrade and surveying for Americans with Disabilities Act web and public application compliance. The 2018 budget includes funding for the continuation of the IT upgrades and replacements and public facilities communications programs, completion of the open data dashboard and analytics tool, and the second phase of the City Assessor modernization project.[2] The total adopted budget for 2018 is $9,188,800.[3]

III. Audit Conclusions and Recommendations

Overall, the audit concluded that the controls in place over physical, IT environmental, data-back up and offsite storage procedures are adequately designed and operating effectively. However, gaps exist in the operational effectiveness of system restoration and data center access controls. This report identifies three recommendations to address these issues.

1. Perform and document periodic physical-access reviews.
2. Enhance the business continuity test, training, and exercise program activity, documentation, and policy.
3. Repair or replace the cooling system's back-up power generator to meet contingency requirements.

Additional details regarding the recommendations for improvement are provided in the remaining sections of this report.

A. Physical Access

In accordance with best practice requirements, including FISCAM,[4] access to facilities should be limited to personnel having a legitimate need for access to perform their duties. Management should regularly review the list of persons authorized to have physical access to sensitive facilities,

[2] City of Milwaukee *2018 Plan and Budget Summary*, page 40.
[3] City of Milwaukee *2018 Adopted Detailed Budget*, Department of Administration-Information and Technology Management Division Section beginning on page 15.
[4] See *Federal Information Systems Controls Audit Manual*, page 260.

including contractors and other third parties. In addition, procedures should be implemented to terminate access privileges for terminated or separated employees or contractors.

In conjunction with ITMD management approval, the Department of Public Works' Operations and Maintenance Manager establishes physical access to the ITMD by assigning electronic keycard access to the ITMD Office, Data Center, and Back-up Data Center for all personnel and other authorized employees (i.e., custodial workers and other employees as necessary). An access-permission record of all employees having access to the above referenced locations was provided to Internal Audit and tested for least-privilege access. All access-permission records were tested as necessary to achieve a reasonable level of assurance of the physical access control's current condition. Based on audit testing, it was determined that the number of employees with physical access to the ITMD Office, Data Center, and Back-up Data Center significantly exceeds the number of users needing access for work purposes.

Recommendation 1: Perform and document periodic physical-access reviews.

To strengthen processes and controls surrounding physical access to the ITMD Office, Data Center, and Back-up Data Center management should:

1. Work in conjunction with DPW management to perform periodic, formal physical access reviews for all individuals with access to the ITMD Office, Data Center, and Back-up Data Center for appropriate access levels, including the removal of access for employees separated from City service or transferred to areas that do not require ITMD access. Only ITMD management should have the final approval regarding all access decisions.

2. Retain the documentation evidencing the completion of these periodic reviews, any changes made as a result of the reviews, and management approvals for the two most recent reviews.

B. Business Continuity and Disaster Recovery Planning

Business continuity criteria and standards encompass planning and preparation to ensure that the ITMD Data Center remains functional in case of serious incidents or disasters and is recoverable to an operational state within a reasonably short period of time. As such, business continuity includes three key elements:

- **Resilience**–Critical business functions and supporting infrastructure must be designed in ways that make them materially unaffected by relevant disruptions, such as through the use of redundancy and spare capacity;

- **Recovery**–Arrangements must be made to timely recover or restore critical and less-critical business functions that have failed; and

- **Contingency**–The ITMD Data Center must have a general capability and readiness to cope effectively with the occurrence of any major incidents and disasters, including unforeseen ones. Contingency preparations constitute a last resort response if resilience and recovery arrangements should prove inadequate in practice.

The business-continuity plan is the key document that organizes and brings all these elements into a meaningful focus.

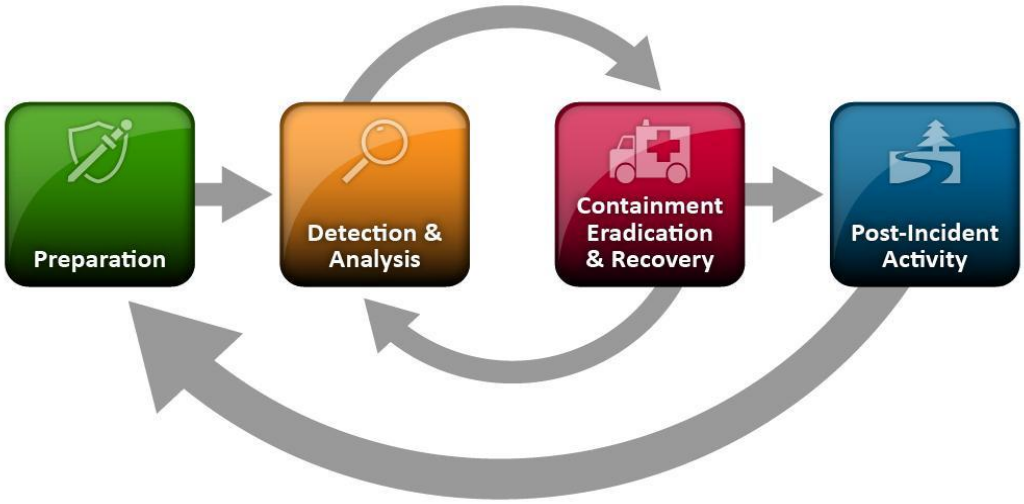
A reliable and effective IT-recovery plan should include the following three elements of IT disaster-recovery control measures:

- **Preventive Measures**–Prevent an event from occurring,
- **Detective Measures**–Detect or discover unwanted events, and
- **Corrective Measures**–Correct or restore the system after an event occurs.

Satisfactory disaster-recovery plan measures dictate that these three types of controls be documented and exercised regularly by testing the plan to the maximum extent possible. The "lessons learned" from actual testing are meant to improve the entire disaster-recovery process.

A high-level overview of the business continuity process is presented below in Figure 2. The figure emphasizes the incorporation of the feedback received through actual testing of the plan into improving the original disaster recovery plan.[5]

Figure 2
Overview of Business Continuity Framework



Business Continuity Testing

The audit included a review and evaluation of the ITMD Data Center business continuity plans to recover from a system outage based on industry best practices and guidelines established by ISACA. The controls over data back-up and offsite storage were tested without exception.

Test, Training, and Exercise Program

Best practice and the standards required by ISACA and FISCAM necessitate enhancement of the TTE program. Specifically, this includes the following:

[5] COBIT 4.1 – Business Continuity Module - Information Systems Audit and Control Association.

- TTE document enhancements or updates,
- Walkthrough and simulation-recovery training with appropriate personnel, and
- Documentation of periodic training activity.

The current ITMD business continuity test, training, and exercise (TTE) program needs improvement regarding documentation, simulation-recovery training and keeping a record of training activity.

Additionally, there should be a TTE policy or Standard Operating Procedure (SOP) that outlines the organization's internal and external requirements associated with training personnel, exercising plans, and testing components and systems. This enhanced TTE practice ensures all applicable employees are up-to-date with implementing business continuity procedures for an important City service.

Recommendation 2: Enhance the business continuity test, training, and exercise program activity, documentation, and policy.

Management should enhance business continuity efforts through the following:

1. TTE document updates;
2. Performance of walkthroughs with appropriate personnel;
3. Conduct simulation recovery training with appropriate personnel;
4. Document periodic training activity; and
5. Development of written policy or standard operating procedure (as is applicable) for the TTE program that outlines the organization's internal and external requirements associated with training personnel, exercising plans, and testing of components and systems.

Additionally, testing the application contingency plan is essential to ensure it will function as intended when activated for an emergency. This enhanced TTE practice helps to ensure all applicable employees are up-to-date with implementing business continuity procedures for critical City services. Ongoing simulation recovery training and practice by IT staff members to rapidly restore a system outage is an important part of the business continuity program.

Cooling System's Back-up Power Generator

ISACA standards recommend that data centers have an adequate back-up power supply to ensure all processing activities are functional in case of the loss of the primary power supply, and processing is recoverable to an operational state within a reasonably short period. As a basis for this audit, current processes, procedures and controls within the ITMD were compared to a best practice relevant controls testing program.

In November of 2016, the Data Center's cooling system back-up generator, located in the 809 N Broadway loading dock area, failed and was unable to return to operable service. The generator is an important component of the continuity plan as it delivers power to the computer room air conditioner (CRAC) units that provide air conditioning within the server rooms. In the event of a main power failure, the server equipment may need to be powered down to prevent overheating and damage to the computing equipment.

This condition may pose a risk of a service outage or service limitations resulting in delayed or unfulfilled citizen services, decreased citizen satisfaction and reputational damage. There is also a nominal risk of equipment damage due to inoperability of the back-up generator needed for adequate cooling of the ITMD Data Center. The cause of the situation is an aging generator, which is nearing the end of its useful life. The generator was installed in 1999 and is approximately 18 years old.

Recommendation 3: Repair or replace the cooling system's back-up power generator to meet contingency requirements.

As contingency planning is critical to ensuring key operations continue to function when unexpected events occur, ITMD management should:

- Collaborate with DPW to develop and implement a permanent, and reliable, emergency power supply solution that enhances contingency planning, and
- Expedite repairing or replacing the emergency back-up generator and keep City leadership and Internal Audit apprised of the remediation in an ongoing manner.

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

May 24th, 2018

Adam Figon
Audit Manager
City Comptroller's Office
City Hall, Room 404
Milwaukee, WI 53202

RE: DataCenter Audit

Mr. Figon,

The ITMD's response to the three recommendations is as follows:

1. Perform and document periodic physical-access review.

   ITMD has established a procedure to request physical access reports for the datacenter in January and July of every year. The reports will be reviewed by ITMD management and requests for changes will be submitted to the DPW Facilities Manager.

2. Enhance the business continuity test, training, and exercise program activity, documentation, and policy.

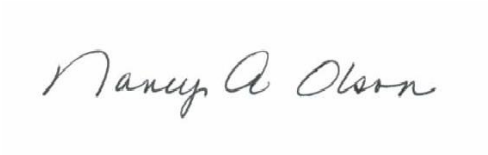
   Up until 2018, ITMD has been without a position dedicated to IT security. The position requested in the budget is expected to be filled next month and activities such as Standard Operating Procedures (SOP) and policies will be assigned. Ultimately, ITMD sees the benefits of exercises, training and testing, but limitations of resources prevent this from happening at this time. Status update available by 12/31/18.

3. Repair or replace the cooling system's back-up power generator to meet contingency requirement.

   ITMD has met with DPW and has been briefed on the plan DPW has for designing a solution for the backup generator. ITMD would like to note that this generator only provides power for the cooling for the data center. Since the implementation of cloud solutions, the cooling needs of the division has been greatly reduced. ITMD appreciates the approach DPW has taken to review the needs prior to the design of a solution. Loss of cooling in the datacenter in the meantime could be handled with air circulation and portable cooling units, making this a low risk. Status update available by 12/31/18.

Suite 400, 809 North Broadway, Milwaukee, Wisconsin 53202. Phone (414) 286-5511

Sincerely,



Nancy A Olson
Chief Information Officer

City of Milwaukee

Department of Public Works

Ghassan Korban, P.E.
Commissioner of Public Works

June 5, 2018

Mr. Adam Figon
Audit Manager
Comptroller's Office
200 East Wells, Room 404
Milwaukee, WI 53202

Dear Mr. Figon:

Subject: Response to Audit of ITMD Data Center Controls – Recommendation 3

The Department of Public Works, Bridges and Buildings (B&B) appreciates the opportunity to work with the Comptroller's office and the Information Technology Management Division (ITMD) regarding the subject audit dated May, 31, 2018 and offers the following response.

Recommendation 3: Repair or replace the cooling system's back-up power generator to meet contingency requirements.

B&B currently has an engineering consultant under contract to study the current electrical system serving the ITMD equipment loads including the cooling system. The electrical needs for ITMD have changed dramatically over the last 18 years, since the emergency generator was installed. This study will provide information necessary to determine the appropriate path forward to provide ITMD with reliable back-up emergency power.

Currently repairs are scheduled for the week of June 10th to return the generator to working order.

Please feel free to contact Mr. Thomas Tarkowski of my staff at extension 3295 if you need additional information.

Sincerely,

Ghassan Korban, P.E.
Commissioner of Public Works

TT:tt

C: C. Liberto
T. Tarkowski
A. Hilgendorf
Central File

Frank P. Zeidler Municipal Building, 841 N. Broadway, Milwaukee, Wisconsin 53202
I:\Greene\Audit response memo.doc Administration, Room 501 (414) 286-3703 ♦ Fax (414) 286-3953 ♦ TDD (414) 286-2025
Contract Administration, Room 506 (414) 286-3314 ♦ Fax (414) 286-8110 ♦ www.city.milwaukee.gov/mpw

MILWAUKEE

Martin Matson
Comptroller

Aycha Sirvanci, CPA, CIA
Deputy Comptroller

Toni Biscobing
Special Deputy Comptroller

Rocklan Wruck, CPA
Special Deputy Comptroller

Office of the Comptroller

June 13, 2018

Honorable Tom Barrett, Mayor
The Members of the Common Council
City of Milwaukee
Milwaukee, WI 53202

Dear Mayor and Council Members:

With this letter, the Office of the City Comptroller acknowledges receipt of the preceding report, which communicates the results of the audit of Information and Technology Management Division's (ITMD) Data Center Controls. I have read the report and support its conclusions. Implementation of the stated recommendations will help improve City processes.

As the City Comptroller, I was not involved in any portion of the work conducted in connection with the audit. At all times, the Internal Audit Division worked autonomously in order to maintain the integrity, objectivity, and independence of the audit, both in fact and in appearance.

Sincerely,

Martin Matson

Martin Matson,
Comptroller

City Hall, Room 404, 200 E. Wells Street, Milwaukee, WI 53202 • Phone (414) 286-3321 • Fax (414) 286-3281
www.milwaukee.gov/comptroller