Audit of Municipal Court Data Center Controls

MARTIN MATSON
City Comptroller

ADAM FIGON
Audit Manager

City of Milwaukee, Wisconsin

December 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

December 12 , 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 Municipal Court data center controls. The scope of the audit included the Municipal Court data center's physical, environmental, and backup control activities and included the alternate data processing site. The time period covered includes the current state of operations and one complete data backup 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's physical and IT environmental controls are compliant with department policy, best practice criteria and standards outlined by the Information Systems Audit and Control Association (ISACA), and

2. Assess whether the data center's controls over data backup, 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 access and the IT environment are adequately designed and operating effectively. However, gaps exist in the operational effectiveness of disaster recovery and business continuity planning, policy and procedure, and key personnel retention. This report identifies five 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 Municipal Court Data Center Controls

Appreciation is expressed for the cooperation given to the auditors by the personnel of the Municipal Court .

Sincerely,

Adam Figon

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 Municipal Court Data Center's physical, environmental and backup control activities and includes the alternate data processing site. The time period covered includes the current state of operations and one complete data backup cycle.

Audit activities consist of process walkthroughs, observations, review of policies and procedures and testing of controls. During the performance of these audit activities, the data center's controls were evaluated using the environmental and backup control standards as 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's 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's controls over data backup, 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 Municipal Court data center. To establish appropriate evaluation criteria for this audit, controls and procedures specific to the Municipal Court data center were compared to a best practice based

controls testing program. The audit program was developed using standards from ISACA, the Federal Information Systems Controls Audit Manual (FISCAM), and the National Institute of Standards and Technology (NIST). ISACA, FISCAM, and NIST present a methodology for performing information system control audits of federal and other governmental entities in accordance with professional standards as presented in Government Auditing Standards, (also known as the "Yellow Book") and were used as reference and program development guides for the planning of this audit. The audit program and procedures also included elements from best practice criteria from COBIT[1], COSO[2], and NIST 800-14, 800-53 (Revision 4), 800-84. 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 Municipal Court Administrative Office and Municipal Court data center, based on the principle of least privilege;
- Assessment of environmental controls to protect against the risk of damage from fire, water, temperature and humidity irregularities, and unauthorized persons;
- Assessment of data backup, offsite storage, and system restoration procedures; and
- Evaluation of the business continuity plans to recover from a service outage.

II. Organization and Fiscal Impact

Municipal Court Mission[3]

The Municipal Court's mission is to safeguard the legal rights of individuals, protect the public interests, and enhance public safety through the timely adjudication of cases. To fulfill its mission, the Municipal Court employs three duly elected Municipal Judges as well as twenty-nine

[1] Control Objectives for Information and Related Technology (COBIT)
[2] Committee of Sponsoring Organizations of the Treadway Commission - 2013 (COSO)
[3] Information for the Municipal Court Mission Section was taken from the *City of Milwaukee 2018 Budget*.

supporting staff members. Municipal Court implements strategies including using technology to streamline operations and reduce cost, especially in the area of case management.

Municipal Court Data Center and Technology Team

The Municipal Court maintains their own data center that includes server racks and cabling, server equipment, and extensive environmental controls. The data center is the back bone of the technology operations which include network infrastructure, software management, and desktop servicing. To support their technology operation, the Chief Court Administrator, with the help of the Assistant Court Administrator, oversee the positions of IT Support Services Supervisor/Network Manager; IT Support Specialist-Senior; and Programmer Analyst. A highly functional technology operation makes it possible for the Municipal Court to process between 60,000 and 180,000 cases per year in a timely manner. Corresponding annual revenues from the cases range from between $4 and $6 million with annual expenses in the range of $3 million.

III. Audit Conclusions and Recommendations

The audit concluded that the controls in place over physical access and the IT environment are adequately designed and operating effectively. However, gaps exist in the operational effectiveness of disaster recovery and business continuity planning, policy and procedure, and key personnel retention. This report identifies five recommendations to address these issues.

1. Produce and store backup data tapes.
2. Enhance the business continuity test, training, and exercise program policy, documentation, and activity.
3. Develop and implement a plan to relocate the backup data recovery site outside of a proximity of ten miles.
4. Develop and maintain written policies and procedures for all Technology Department operations.
5. Collaborate with DER to modify the IT Manager recruitment parameters to meet Municipal Court's needs.

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

A. Physical Access and Environmental Controls

Physical Access

Access to facilities should be limited to personnel having a legitimate business need for access to perform their job duties and based on the least privilege principle. Management should periodically review the list of persons authorized to have physical access to sensitive facilities, including contractors, maintenance and other parties. In addition, procedures should include the timely termination of access privileges for separated employees and contractors[4].

Municipal Court's physical access controls were thoroughly examined to ensure adequate controls existed and were operating effectively. The examination included, 1) Obtaining a complete list of personnel with proximity card access to both the Municipal Court Administrative Office area and the data center, 2) verifying each person on the list was entitled to access based on the principle of least privilege, and 3) confirming that a procedure was in place for the periodic review of personnel with physical access and that a review was being performed by management in a timely manner.

Based on the examination of physical access to the Municipal Court Administrative Offices and data center, it was determined strong controls exist and are operating effectively.

Environmental Controls

Environmental controls prevent or mitigate potential damage to facilities and interruptions in service. Examples of environmental controls include;

- fire extinguishers and fire-suppression systems;
- fire alarms;
- smoke detectors;
- water detectors;
- emergency lighting;

[4] U.S. Government Accountability Office, *Federal Information Systems Controls Audit Manual (FISCAM)*, 2009, Page 260.

- redundancy in air cooling systems;
- backup power supplies;
- existence of shut-off valves and procedures for any building plumbing lines that may endanger processing facilities;
- processing facilities built with fire-resistant materials and designed to reduce the spread of fire; and,
- policies prohibiting eating, drinking, and smoking within computer facilities.

Environmental controls can diminish the losses from some interruptions such as fires or prevent incidents by detecting potential problems early, such as water leaks or smoke, so that they can be remedied. Also, uninterruptible or backup power supplies can carry a facility through a short power outage or provide time to backup data and perform orderly shut-down procedures during extended power outages.[5]

An observation tour and review of the physical security and environmental controls of the Municipal Court data center was conducted along with a discussion of safeguards with Municipal Court staff. The observation tour noted the following key controls: 1) a climate controlled environment (temperature, humidity, sunlight); 2) fire extinguishers readily available; 3) a backup generator system available and evidence of recent test; 4) a power surge protection system; 5) an uninterrupted power supply available; 6) computer room is located above the first floor (lowers flood risk); 7) computer room is located on an inner wall (lowers tornado risk); 8) security cameras are located at select entrances; and 9) armed security officers are on premise on a 24/7 basis with a security desk operated during normal business hours.

Based on the observation tour and review of the Municipal Court data center the physical security and environmental controls are designed properly and operating effectively.

[5] U.S. Government Accountability Office, *Federal Information Systems Controls Audit Manual (FISCAM)*., 2009, Page 320.

B. Backup Data Tapes

Best practice indicates file backup procedures should be designed so that a recent backup data copy is always available (FISCAM Contingency Planning 2.1).

Municipal Court does not produce and store backup tapes. In the past, Municipal Court had a policy of producing backup tapes, but the policy was discontinued. Though electronic file backups are available from the Municipal Court Nimble Storage file backup system, restoring the policy of utilizing backup tapes would offer an added layer of backup file storage for key systems and would promote uniformity in the backup tape policy between ITMD and the Municipal Court.

Recommendation 1: Produce and store backup data tapes.

As multiple layers of data backup are the best way to ensure a viable data backup is always available, Municipal Court should develop and implement a new, up-to-date procedure that addresses the following:

- Creation of backup tapes.
- Storage and archiving of backup tapes.
- Cycling of backup tapes.

Municipal Court uses the Information Technology Management Division's (ITMD) main data center as the backup data center for Municipal Court data servers. In order to develop consistency between ITMD and the Municipal Court, Municipal Court should consider partnering with ITMD to have backup tapes created, stored, and archived as part of ITMD's standard backup tape process. Partnering with ITMD should prove effective as ITMD currently has a vendor contract in place with Iron Mountain for backup tape transport and storage.

C. Business Continuity and Disaster Recovery Planning

Business continuity criteria and standards encompass planning and preparation to ensure that the Municipal Court 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 Municipal Court 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:

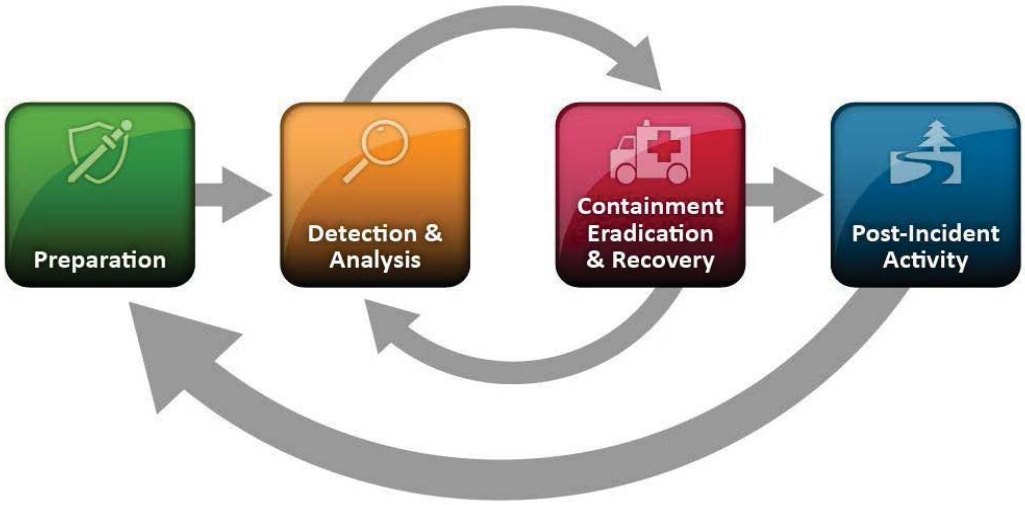
- **Preventive Measures**–Prevent an event from occurring,
- **Detective Measures**–Detect or discover unwanted events, and
- **Corrective Measures**–Correct or restore the system after an event occurs.

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.[6]

Figure 2

Overview of Business Continuity Framework



Business Continuity Testing

The audit included a review and evaluation of the Municipal Court 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 backup and offsite storage were adequate with exception for the *backup data tapes* and *backup data center proximity* which are addressed as separate findings in this report.

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

Test, Training, and Exercise Program (TTE)

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

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

The current Municipal Court 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 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 policy; documentation; and activity.

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.
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.

Backup Data Center Proximity

Best practice indicates a distance of ten to twenty miles from the primary data center as an acceptable distance for a recovery site. In determining the appropriate distance for a recovery site, an entity should consider if there is enough distance between your primary site and recovery site to escape the same set of threats (i.e.; flooding, tornado, power grid failure, etc.).

Municipal Court uses the Information Technology Management Division's (ITMD) main data center as the backup data center for Municipal Court data servers. The physical distance between the Municipal Court location (951 N Lovell) and the ITMD location (809 N Broadway) is approximately .63 miles or 8 city blocks away.

The benefits and drawbacks of City-wide backup data center consolidation should also be considered in order to maximize operational efficiency while simultaneously addressing risk concerns.

Recommendation 3: Develop and implement a plan to relocate the backup data recovery site outside of a proximity of ten miles.

- For cost and operational efficiency and enhancement; the Municipal Court should collaborate with ITMD and other City technology departments (Water, Library, etc.) to develop a consolidated backup data recovery site that is at least ten miles away from the closest data center and has strong physical security and environmental controls.

D. Policy and Procedure

According to best practice requirements, including the 2013 COSO Framework–Principle 12: Management should implement control activities through policies that establish what is expected and through procedures that put policies into action.

The Municipal Court Technology Department adequately utilizes various policies and procedures. However, there were four occurrences of a procedure not being reviewed for updates by

management on a periodic basis. Reviewing policies and procedures on a periodic basis will ensure relevancy, as well as secure succession of process knowledge.

Recommendation 4: Develop and maintain written policies and procedures for all Technology Department operations.

Municipal Court should:

- Implement a formal periodic review process that includes evidencing review and updates with management signature and date.
- Store all IT policies and procedures in a centralized, easily accessible location to facilitate accessibility and departmental cohesion.

E. Turnover in Technology Manager Position

Best practices[7] indicate a number of areas can be especially powerful in enabling an organization to achieve its personnel retention goals. These areas include:

- ***Compensation and rewards***

  Pay levels and satisfaction can be predictors of an employee's decision to leave the organization; however, a company has three possible strategies in approaching pay:

  1. Lead the market with respect to compensation and rewards
  2. Tailor rewards to individual needs in a person-based pay structure, and
  3. Explicitly link rewards to retention (e.g., tie vacation hours to seniority, offer retention bonuses to longer-term employees, or link defined benefit plan payouts to years of service).

- ***Recruitment***

  Timely recruitment practices can strongly influence turnover, and considerable research shows that presenting applicants with a realistic and timely job preview during the recruitment process has a positive effect on retention of those new hires.

[7] Society for Human Resource Management (SHRM), *Managing for Employee Retention,* May 24, 2018

- ***Socialization***

  Turnover is often high among new employees. Socialization practices—delivered via a strategic onboarding and assimilation program—can help new hires become embedded in the company.
- ***Training and development***

  If employees are not given opportunities to continually update their skills, they are more inclined to leave.
- ***Employee engagement***

  Engaged employees are satisfied with their jobs, enjoy their work and the organization, believe that their job is important, have respect for their company, and believe that their employer values their contributions.

Over the last five years Municipal Court has had four different technology heads with an average tenure of between 1 and 1.5 years. During the hiring process for the most recent IT Manager, 14 candidates submitted an application; however, five withdrew due to salary constraints and three withdrew after accepting another job offer while traversing the City's recruitment process.

A number of causes can be attributed to the inability to attract and retain top IT management personnel including:

- Inability to recruit top talent in the highly competitive technology industry due to constraints in offering competitive compensation.
- Qualified candidates find other jobs while waiting to hear back from the City due to a protracted hiring process.
- Municipal Court's unique need for a candidate who is able fill multiple roles (technology and administrative based) within the Municipal Court administrative team.

Recommendation 5: Collaborate with DER to modify the IT Manager recruitment parameters to meet Municipal Court's needs.

In order to meet the recruitment and retention needs for a qualified technology head, Municipal Court should:

- Exempt the IT Support Services Supervisor and/or Network Manager positions as necessary.
- Work with DER to allow for hiring qualified personnel above the midpoint of the grade range for the positions of IT Support Services Supervisor and/or Network Manager as necessary.

CITY OF MILWAUKEE
MUNICIPAL COURT

Derek C. Mosley, Presiding Judge
Branch 2

Valarie A. Hill, Judge
Branch 1

Phillip M. Chavez, Judge
Branch 3

Sheldyn M. Himle
Chief Court Administrator

Jane E.T. Islo
Assistant Court Administrator

November 29, 2018

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

RE: Response to the Audit of Municipal Court Datacenter Controls

Dear Mr. Figon:

The Milwaukee Municipal Court values the work of your office and staff in conducting the recent audit of Municipal Court's Data Center Controls. As all case records of the Municipal Court are stored electronically, every aspect of the technology required to house records and maintain Court operations is vital. Therefore, we appreciate the objective scrutiny of our procedures.

Recommendation 1: Produce and store backup data tapes.

Municipal Court had previously been producing daily backup tapes and sending tapes offsite twice each week. A couple years ago, this practice was ended at the direction of the then-IT manager who had been under the impression that they were no longer necessary. The Court will re-implement this process and codify it as a best practice and standard procedure. This implementation will be included in the current CATS Upgrade Project, the entirety of which is scheduled to conclude at the end of 2019.

Target Completion Date: June, 2019

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

Management understands the need for better documentation, standardized training, and routine testing exercises for components and systems. The challenge to establishing this has been directly related to a lack of consistent leadership in the IT section. As noted in the audit, there have been four different managers in the past five years. Regardless, as described in the audit, the Court will move to enhance business continuity efforts by:

- Creating and maintaining a test, training and exercise (TTE) plan
- Performing walkthroughs
- Conducting simulation recovery training
- Documenting periodic training activity
- Developing written policies or standard operating procedure (as is applicable) for the TTE program, outlining internal and external requirements associated with training personnel, exercising plans, and institute testing of components and systems.

951 North James Lovell Street, Milwaukee, Wisconsin 53233-1449. Phone (414) 286-3800, FAX (414) 286-3615.
www.municourt.milwaukee.gov

This will also be included as part of the Court's CATS Upgrade Project.

Target Completion Date: December, 2019

Recommendation 3: Develop and implement a plan to relocate the backup data recovery site outside of a proximity of ten miles.

While the Court does have a backup data recovery site, it is not more than ten miles away. As recommended, the Court intends to collaborate with other City departments to develop a consolidated backup data recovery site that is at least ten miles away from the closest data center and has strong physical security and environmental controls. As with the first two recommendations, the Court will include this as part of the CATS Upgrade Project.

Target Completion Date: December, 2019

Recommendation 4: Develop and maintain written policies and procedures for all Technology Department operations.

As recommended Municipal Court will:

- Implement a formal periodic review process that includes evidencing review and updates with management signature and date.
- Store all IT policies and procedures in a centralized, easily accessible location to facilitate accessibility and departmental cohesion.

Target Completion Date: June, 2019

Recommendation 5: Collaborate with DER to modify the IT Manager recruitment parameters to meet Municipal Court's needs.

As recommended, the Court has already begun to work with DER to consider the best options to modify the IT manager recruitment parameters and to quickly move to recruit.

Target Completion Date: August, 2019

Milwaukee Municipal Court will work toward completing work on all five recommendations, as outlined here. Because our ability to meet some of these projected deadlines is not completely within our control, we will inform the Comptroller's office of impediments that arise.

Sincerely,

Sheldyn M. Himle
Chief Court Administrator

951 North James Lovell Street, Milwaukee, Wisconsin 53233-1449. Phone (414) 286-3800, FAX (414) 286-3615.
www.municourt.milwaukee.gov

MILWAUKEE

Martin Matson
Comptroller

Aycha Sawa, CPA, CIA
Deputy Comptroller

Office of the Comptroller

Toni Biscobing
Special Deputy Comptroller

Rocklan Wruck, CPA
Special Deputy Comptroller

November 30th, 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 Municipal Court 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