



**Audit of the Milwaukee Fire
Department Data Center
Controls**

MARTIN MATSON
City Comptroller

AYCHA SAWA
Interim Audit Manager

City of Milwaukee, Wisconsin

November 2019

Table of Contents

Transmittal Letter	1
Audit Report Highlights	2
I. Audit Scope, Objectives, and Methodology	3
II. Organization and Fiscal Impact	5
III. Audit Conclusions and Recommendations	5
A. Business Continuity and Disaster Recovery Planning	6
<u>Recommendation 1</u> : Establish business continuity test, training, and exercise program policy, documentation, and activity	8
<u>Recommendation 2</u> : Produce and store backup data tapes	9
<u>Recommendation 3</u> : Develop and implement a plan to relocate the backup data recovery site outside of a proximity of ten miles	9
B. Environmental Controls	10
<u>Recommendation 4</u> : Enhance fire prevention controls	10
<u>Recommendation 5</u> : Establish policy and procedure for temperature and humidity controls	11
<u>Recommendation 6</u> : Enhance space utilization including reduction or clearing of clutter	11
<u>Recommendation 7</u> : Enhance flood prevention controls	11
<u>Recommendation 8</u> : Eliminate windows on exterior walls	11

C. Policy and Procedure	12
<u>Recommendation 9:</u> MFD should develop its own set of data center policies and procedures specifically for MFD , independent of MPD	12
D. Physical Access	13
<u>Recommendation 10:</u> Perform and document periodic physical access reviews	13
<u>Recommendation 11:</u> Establish policy and procedure requiring the use of visitor logs at both data center locations	14
V. Management Response from the Fire Department	15
VI. Comptroller’s Acknowledgement of Receipt	20

Martin Matson
Comptroller

Aycha Sawa, CPA, CIA
Deputy Comptroller



Toni Biscobing
Special Deputy Comptroller

Rocklan Wruck, CPA
Special Deputy Comptroller

Office of the Comptroller

November 13, 2019

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 Milwaukee Fire Department Data Center Controls. The scope of the audit included the Milwaukee Fire Department (MFD) data center's physical security, environmental, and backup control activities including the alternate data processing site. During the course of the audit it was necessary to expand the scope to include the Milwaukee Police Department (MPD) as MPD owns the facilities that house the servers. 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 designed adequately 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 the Information Systems Auditing and Control Association (ISACA), Federal Information System Controls Audit Manual (FISCAM), and the National Institute of Standards and Technology (NIST); and,
2. Assess whether the data center 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, FISCAM and NIST.

The audit concluded that the controls in place over physical access to be adequate. However, controls over disaster recovery and business continuity planning, environment management, and policy and procedure were found to be deficient and in need of prompt attention. This report identifies 11 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.

Appreciation is expressed for the cooperation extended to the auditors by the personnel of the Milwaukee Fire Department.

Sincerely,

A handwritten signature in black ink, appearing to read "Aycha Sawa".

Aycha Sawa, CPA, CIA
Interim Audit Manager

AS:bhd



AUDIT REPORT HIGHLIGHTS

Audit of the Milwaukee Fire Department Data Center Controls

WHY WE DID THIS AUDIT

City data centers were identified as a high risk area in the Citywide IT Risk Assessment. The **MFD data centers are the foundation for MFD operations**, and business continuity is essential to ensuring ongoing services to citizens. Continuity involves the ability to restore lost data easily and to minimize or eliminate system downtime from a business disruption event that can lead to lost productivity, costly data recovery and severe service interruptions to citizens.

OBJECTIVES

The objectives of the audit were to assess whether the data center physical and IT environmental controls, and controls over data backup, offsite storage and system restoration were in compliance with department policy and best practice criteria and standards.

BACKGROUND

MFD's emergency response system is housed in joint data center facilities shared with the Milwaukee Police Department. While the data center facilities are shared, MFD administers its own technology operations encompassing network infrastructure, software management, and desktop servicing, with an annual budget of roughly \$700,000. MFD IT staff include IT Manager, Application Analyst, IT Support Specialist, and 3 Systems Analysts.

OVERVIEW

The **audit concluded that control deficiencies exist in every area tested**. Prompt attention is needed to address these deficiencies including strengthening controls over disaster recovery and business continuity planning, environment management, and policy and procedure. This report includes 11 recommendations to address these issues.

WHAT WE FOUND

Business Continuity-Test, Training, and Exercise: MFD does not conduct periodic test, training and exercise programs for disaster recovery and business continuity planning. Best practice dictates that planning, preparation and practice regularly occur to ensure that a 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.

Data Backup: At the time of the audit, there were no backup tapes (or backup tape alternative) produced and stored by MFD, although Internal Audit was advised that MFD was in the process of negotiating a contract with Amazon Web Services for a solution. Best practice establishes file backup procedures should be designed so that a recent copy is always available. In addition, multiple layers of backup media are the safest way to ensure a viable backup is always available.

Data Center Proximity: MFD uses a server room located in the Police Department's Radio Shop as its backup data center. The physical distance between MFD's primary data center and the Radio Shop location is only approximately 0.9 miles away, which is insufficient to protect against natural disasters such as a power outage due to a storm or tornado. Best practice establishes a distance of at least 10 to 20 miles from the primary data center to be an acceptable distance for a recovery site.

Environmental Controls: MFD had deficient fire suppression, temperature and humidity, room capacity management, and flood protection controls. Of particular importance is the lack of adequate fire prevention controls at the backup sever room location. Best practice establishes that environmental controls should be maintained to diminish the losses from interruptions such as fires or prevent incidents by detecting potential problems early, such as water leaks or smoke, so that they can be remedied.

(Detail on all 11 recommendations can be found in the Audit Conclusions and Recommendations section of this report.)

I. Audit Scope, Objectives, and Methodology

Scope

The scope of the audit encompassed the Milwaukee Fire Department (MFD) data center's physical security, environmental and backup control activities, including the alternate data processing site. The time period covered included the current state of operations and one complete data backup cycle.

During conversations with MFD and on the tour of the server rooms shared by MFD and the Milwaukee Police Department IT Division (MPD), it was discovered that many server room controls are under the ownership of MPD. As a result, any audit recommendations to strengthen server room controls require a combined effort from both MFD and MPD. Therefore, Internal Audit expanded the audit's scope to include MPD's participation in the presentation of findings and recommendations, reporting, and remediation efforts.

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 the Information Systems Auditing and Control Association (ISACA), Federal Information System Controls Audit Manual (FISCAM), and the National Institute of Standards and Technology (NIST); and,
2. Assess whether the data center 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, FISCAM, and NIST.

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 MFD data center. To establish appropriate evaluation criteria for this audit, controls and procedures specific to the MFD data center were compared to a best practice based controls testing program. The audit program was developed using criteria outlined by ISACA, FISCAM, and NIST. These best practice standards 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”), which was used as a reference and program development guide for the planning of this audit. The audit program and procedures also included elements from best practice criteria Control Objectives for Information and Related Technology (COBIT), Committee of Sponsoring Organizations of the Treadway Commission -2013 (COSO), and NIST 800-14, 800-53 (Revision 4), 800-84.

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 District 3 and Radio Shop data centers, 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 disaster recovery and business continuity plans to recover from a service outage.

II. Organization and Fiscal Impact

Milwaukee Fire Department Mission¹

MFD's mission is to prevent loss of life, limit fire related property damage, and improve the chances of survival from life threatening medical circumstances. To achieve its mission a well-functioning emergency response system is indispensable. The MFD emergency response system is housed in joint data center facilities shared with MPD. While the data center facilities are shared, the MFD administers its own technology operations encompassing network infrastructure, software management, and desktop servicing. To support its technology operation, the positions of Fire IT Manager, Systems Analysts, IT Support Specialists, and Functional Applications Analyst are maintained. The technology operations are strongly dependent upon a well maintained and functioning data center.

The MFD provides timely emergency response to Milwaukee's 600,000 citizens. In order to provide a high level of emergency service, MFD has 871 authorized full-time equivalent (FTE) positions. The positions can be subdivided by Fire Operations (706), Fire Support Services (83), and Fire EMS Training and Education (82 FTEs). Total budgeted payroll and fringe benefits are \$104 million or approximately 93% of the total budget. Budgeted annual expenses for 2018 and 2019 were \$111 and \$112 million respectively. Budgeted annual revenues from service charges for 2018 and 2019 were \$6.5 and \$6 million respectively.

III. Audit Conclusions and Recommendations

The audit concluded that the controls in place over physical access to be adequate. However, controls over disaster recovery and business continuity planning, environment management, and policy and procedure were found to be deficient and in need of prompt attention. This report identifies 11 recommendations to address these issues.

1. Establish business continuity test, training, and exercise program policy, documentation, and activity.
2. Produce and store backup data tapes.

¹ City of Milwaukee, 2019 Plan and Budget Summary, pages 85-89

3. Develop and implement a plan to relocate the backup data recovery site outside of a proximity of ten miles.
4. Enhance fire prevention controls.
5. Establish policy and procedure for temperature and humidity controls.
6. Enhance space utilization including reduction or clearing of clutter.
7. Enhance flood prevention controls.
8. Eliminate windows on exterior walls.
9. MFD should develop its own set of data center policies and procedures specifically for MFD, independent of MPD.
10. Perform and document periodic physical access reviews.
11. Establish policy and procedure requiring the use of visitor logs at both data center locations.

To highlight the most important findings, each was assigned a risk rating from high (most risk) to low (least risk) based on Internal Audit's professional judgement.

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

A. Business Continuity and Disaster Recovery Planning

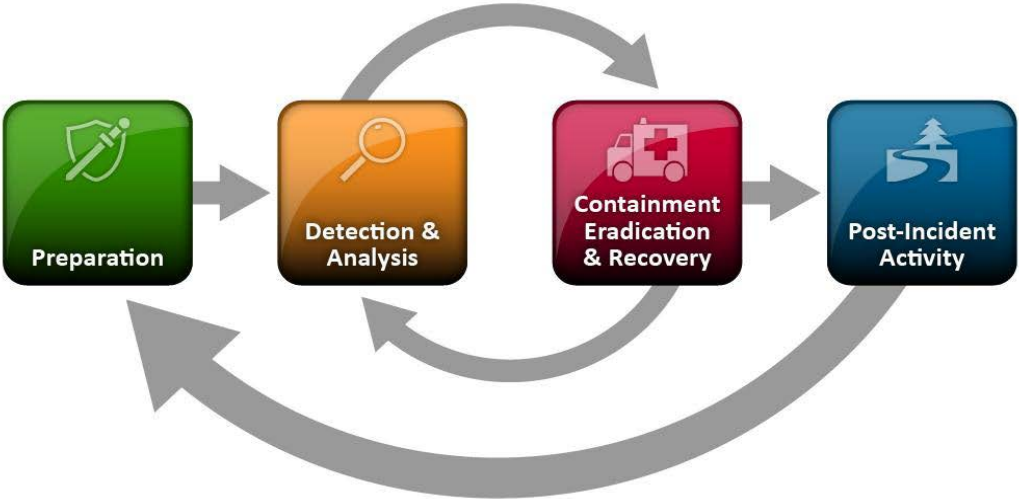
Business continuity criteria and standards encompass planning and preparation to ensure that the MFD data center remains functional in case of serious incidents or disasters and is recoverable to an operational state within a reasonably short period of time. The business continuity plan is the key document that organizes best practice 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.²

Figure 2
Overview of Business Continuity Framework



Business Continuity Testing

The audit included a review and evaluation of the MFD data center business continuity plans to recover from a system outage compared to industry best practices and guidelines established by ISACA. The controls over data backup (with the exception of backup tapes) and offsite storage were adequate. Exceptions were noted for controls related to *test, training and exercise, backup data tapes, and backup data center proximity* which are addressed as separate findings in this report.

² Information Systems Audit and Control Association (ISACA), *COBIT 4.1-Business Continuity Module*.

Test, Training, and Exercise Program (TTE) - Risk Rating: High

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

Recommendation 1: Establish business continuity test, training, and exercise program policy, documentation, and activity to ensure it will function as intended when activated for an emergency, and to ensure all applicable employees are up-to-date with implementing business continuity procedures, including the following elements:

1. Update test, training, and exercise documentation;
2. Perform walkthroughs with appropriate personnel;
3. Conduct simulation recovery training with appropriate personnel;
4. Document periodic training activity; and
5. Develop written policy or standard operating procedure (as applicable) for the test, training and exercise program that outlines the organization's internal and external requirements associated with training personnel, exercising plans, and testing components and systems.

Backup Data Tapes - Risk Rating: High

Best practice establishes file backup procedures should be designed so that a recent copy is always available³. Multiple layers of backup media are the safest way to ensure a viable backup is always available. The layers may include backup tapes, offsite data storage, local data storage devices, and cloud storage services.

³ US Government Accountability Office, *Federal Information Systems Controls Audit Manual (FISCAM)*, CP 2.1

At the time of the audit, there were no backup tapes produced and stored by MFD, although Internal Audit was advised that MFD was in the process of negotiating a contract with Amazon Web Services for a solution.

Recommendation 2: Produce and store backup data tapes.

MFD should implement the backup solution with Amazon Web Services or another provider/solution as soon as possible. Any solution implemented should include:

1. Creating backup tapes or other reliable backup media
2. Storing and archiving of backup tapes or other reliable backup media
3. Cycling of backup tapes or other reliable backup media

Backup Data Center Proximity - Risk Rating: Medium

Best practice establishes a distance of 10 to 20 miles from the primary data center to be an acceptable distance for a recovery site based on the City's geographic region. In determining the appropriate distance for a recovery site, an entity should consider if there is enough distance between the primary site and recovery site to escape the same set of threats (i.e.; flooding, tornado, power grid failure, etc.).

MFD uses a server room located in the MPD's Radio Shop as its backup data center. The physical distance between the MFD's primary data center (2333 N. 49th Street) and the Radio Shop location (4733 W. Vliet Street) is approximately .9 miles away.

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

1. For cost and operational efficiency, MFD should collaborate with other City IT departments to consider developing a joint backup data recovery site that is an appropriate distance from the main data centers and has strong physical security and environmental controls.

B. Environmental Controls

Environmental controls prevent or mitigate potential damage to facilities and interruptions in service. 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.⁴

Fire Prevention - Risk Rating: High

At the time of the walkthrough of the backup data center located at the Radio Shop location, there were deficient fire suppression controls observed at this data center including:

- No smoke detectors.
- No FM-200 fire suppression system or other fire suppression system
- One fire extinguisher, of the two onsite, was last inspected in 2016 while the other was current.

Recommendation 4: Enhance fire prevention controls including:

1. Development and implementation of a complete fire prevention plan at the Radio Shop location.

Temperature and Humidity - Risk Rating: Medium

Facility management has established informal temperature & humidity parameters as follows: Temperature is set at 68F with an alarm point of 73F, and humidity is set at 35%.

MFD has no formal policy and procedure addressing temperature and humidity monitoring and controls. There was no formal monitoring of temperature and humidity levels in the data centers at the time of the audit. Temperature and humidity records could not be produced for the months of our sample. Therefore Internal Audit could not complete its testing sample and arrive at any conclusion regarding temperature and humidity levels during the audit time frame.

⁴ US Government Accountability Office, *Federal Information Systems Controls Audit Manual (FISCAM)*, 2009, CP-2.2

Recommendation 5: Establish policy and procedure for temperature and humidity controls including:

1. Monitoring of temperature and humidity to ensure the server room stays within the established criteria.
2. Retaining temperature and humidity data for periodic reporting and audit review.
3. Implementing best practice temperature and humidity controls.

Room Capacity & Space Efficiency: Clutter - Risk Rating: Medium

Environmental controls for room capacity and space efficiency can diminish the losses from accidents and injury, reduce fire risk, optimize cooling resources, and ensure an optimal clean environment to protect high dollar investments in technology equipment.

Both of the data center locations exhibit clutter within the data centers with more extreme clutter noted at the primary data center at the District 3 location.

Recommendation 6: Enhance space utilization including reduction or clearing of clutter.

Flood Protection - Risk Rating: Medium

For the District 3 data center there was no leak detection system for the data center. In addition, at the Radio Shop server room there was no raised floor, floor drain, or leak detection system.

Recommendation 7: Enhance flood prevention controls including:

1. Installing floor drains, leak detection systems, and raised floors or other compensating controls.

Radio Shop Data Center Exterior Window - Risk Rating: Medium

For security, sound, and environmental management reasons, server rooms should not have windows.

The Radio Shop location is a raised space inside a garage approximately one story off the ground. There are windows on the exterior walls of the space.

Recommendation 8: Eliminate all windows on exterior walls.

C. Policy and Procedure (P&P)

According to best practice requirements, management should implement control activities through policies that establish what is expected and through procedures that put policies into action.⁵

Also, GAO-14-704G Federal Internal Control Standards (the “Green Book”), Principle 12.05 lists the following control activity: Management periodically reviews policies, procedures, and related control activities for continued relevance and effectiveness in achieving the entity’s objectives or addressing related risks. If there is a significant change in an entity’s process, management reviews this process in a timely manner after the change to determine that the control activities are designed and implemented appropriately.

Policy and Procedure - Risk Rating: Medium

MFD Policies & Procedures are seriously deficient as follows:

- Of the 8 general policies recommended by best practices, MFD has not developed 6 (75%) of them.
- The missing P&P are: Access Control, Data Security, Physical Security, Environmental Standards, IT Inventory and Vendor Management, and Data Center Capacity and Upkeep Management. (This should not be considered an all-inclusive list of best practice P&P, but rather, a representative minimum.)
- Of the P&P that exist, there is no evidence of periodic review and update, and no evidence they have been updated since 2011.
- MFD has some general policy, but is lacking in detailed procedures implementing the policies.
- MFD shares data center facilities with MPD and often defers to MPD for P&P. However, MFD cannot produce the MPD P&P to which they defer.

Recommendation 9: MFD should develop its own set of data center policies and procedures specifically for MFD, independent of MPD, including the following:

⁵ Committee of Sponsoring Organizations of the Treadway Commission -2013 (COSO), Principle 12

1. Develop policy for the items recommended by best practices.
2. Implement a formal periodic review process that includes evidencing review and updates with management signature and date.
3. Store all policies and procedures in a centralized, easily accessible location to facilitate accessibility and departmental cohesion.
4. Develop detailed procedures implementing department policies.

D. Physical Access Security

Physical Access Reviews - Risk Rating: Low

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 contractors⁶.

Based on the testing of physical access at District 3, 4 (4% of total) individuals had access privileges that were no longer needed. In addition, testing of physical access at the Radio Shop revealed 3 (or 3.6%) individuals had access privileges that were no longer needed. These same individuals were also on the District 3 Data Center access list.

Recommendation 10: Perform and document periodic physical access reviews

To strengthen processes and controls surrounding physical access to the District 3 and Radio Shop data centers, management should:

1. Perform periodic, formal physical access reviews for all individuals with access to MFD server rooms for appropriate access levels, including the removal of access for employees separated from City service or transferred to areas that do not require access. MPD should have the final approval regarding all access decisions with input from MFD regarding MFD personnel. This review should be performed in addition to, and perhaps simultaneously with, the review that is done of non-MPD department members to MPD facilities.

⁶ US Government Accountability Office, *Federal Information Systems Controls Audit Manual (FISCAM)*, 2009, Page 260.

2. Retain the documentation evidencing the completion of the periodic review, any changes made because of the review, and management approval evidenced by signature and date.

Visitor Logs - Risk Rating: Low

All visitors should be required to sign a visitor's log indicating their name, company represented, reason for visiting, person to see and date and time of entry and departure. Logging typically is at the front reception desk and entrance to the computer room. Before gaining access, visitors should also be required to provide verification of identification such as a driver's license, business card or vendor identification tag. All visitors should be escorted by a responsible employee. Visitors include friends, maintenance personnel, computer vendors, consultants (unless long-term, in which case special guest access may be provided) and auditors.

At the time of the data center tours, no visitor logs were observed and Internal Auditors were not required to sign a visitor log upon entry into the server room at either data center location.

Recommendation 11: Establish policy and procedure requiring the use of visitor logs at both data center locations which requires:

1. All visitors to sign the log and provide proper identification;
2. All visitors to be escorted by a responsible employee.



Fire Department

Mark Rohlfing
Chief

John Schwengel
Assistant Chief
David Votsis
Assistant Chief
Aaron Lipski
Assistant Chief

November 8, 2019

Responses to Audit of Milwaukee Fire Department Data Center Controls Summary of Findings and Recommendations

Finding 1.

Condition: The Milwaukee Fire Department (MFD) does not conduct periodic test, training and exercise programs for disaster recovery and business continuity planning as required by the best practices and standards established by ISACA, FISCAM, and NIST.

Recommendation 1: Establish business continuity test, training, and exercise program policy, documentation, and activity to ensure it will function as intended when activated for an emergency, and to ensure all applicable employees are up-to-date with implementing business continuity procedures, including the following elements:

1. Test, training, and exercise 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 applicable) for the test, training and exercise program that outlines the organization's internal and external requirements associated with training personnel, exercising plans, and testing components and systems.

Response: The Milwaukee Fire Department's Technical Services division does take the appropriate measures to ensure the systems are backed up and secured. Restores are conducted on a regular basis to ensure the functionality of the system. Further testing is a part of our integrated strategic plan for the future. We plan to implement the recommended updates/changes by December 31, 2021 (Pending Budgetary Approval).

Finding 2.

Condition: At the time of the audit, there were no backup tapes produced and stored by the Fire Department, although Internal Audit was advised that the Fire Department was in the process of negotiating a contract with Amazon Web Services for a solution.

Recommendation 2: Produce and store backup data tapes.

Fire Department should implement the backup solution with Amazon Web Services or another provider/solution as soon as possible. Any solution implemented should include:

- Creating backup tapes or other reliable backup media
- Storing and archiving of backup tapes or other reliable backup media

Cycling of backup tapes or other reliable backup media

Response: The Milwaukee Fire Department's Technical Services division does daily backups of all critical systems. The backups are maintained for a minimum of 30 days. In addition, backup jobs are replicated to the radio shop every four hours. Part of our integrated strategic plan is move our offsite backup to AWS Cloud. Our goal is to have our offsite backups replicated to the Cloud by December 31, 2020 (Pending Budgetary Approval).

Finding 3.

Condition: MFD uses a server room located in the MPD's Radio Shop as its backup data center.

The physical distance between the MFD's primary data center (2333 N. 49th Street) and the Radio Shop location (4733 W. Vliet Street) is approximately .9 miles away.

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, MFD should collaborate with other City technology departments to develop a joint backup data recovery site that is an appropriate distance in proximity to the main data centers and has strong physical security and environmental controls.

Response: The Milwaukee Fire Department is aware of the risks that come with using the Radio Shop as their offsite backup location. Part of our integrated strategic plan is move our offsite backup to AWS Cloud by December 31, 2020 (Pending Budgetary Approval).

Finding 4.

Condition: Radio Shop Fire Risk:

- There were deficient fire suppression controls observed at this data center including:
 - No smoke detectors.
 - No sprinkler or halon or other fire suppression system

One fire extinguisher, of the two onsite, was last inspected in 2016 while the other was current.

Recommendation 4: Enhance fire prevention controls including:

Development and implementation of a complete fire prevention plan at the Radio Shop location.

Response: The maintenance of the fire suppression controls for the Radio Shop fall under the responsibility of the Milwaukee Police Department. The Milwaukee Police Department has begun remediating several of these findings. The recommended changes will take until December 31, 2022 to implement (Pending Budgetary Approval).

Finding 5.

Condition: There is no formal policy & procedure addressing temperature & humidity monitoring and controls.

- There was no formal monitoring of temperature and humidity levels in the data centers at the time of the audit.
- Temperature & humidity records could not be produced for the following months of our sample: January, April and June, 2019 and therefore Audit could not complete its testing sample and arrive at any conclusion regarding temperature & humidity levels during the audit time frame.

Recommendation 5: Establish policy and procedure for temperature and humidity controls including:

- Monitoring of temperature and humidity to ensure server room stays within criteria established.
- Retaining temperature and humidity data for periodic reporting and audit review.
- Implementing best practice temperature and humidity controls.

Response: The Milwaukee Police Department is working on remediating this finding. It is estimated that they will have the recommended changes implemented by December 31, 2023 (Pending Budgetary Approval).

Finding 6.

Condition: Both of the data center locations exhibit clutter within the data centers with more extreme clutter noted at the primary data center at the District 3 location.

Recommendation 6: Enhance space utilization including reduction or clearing of clutter.

Response: The data center located at District 3 is the responsibility of the Milwaukee Police Department. The Milwaukee Police Department have a long term strategic plan to reduce the clutter in that space. They estimate to have the recommended changes implemented by December 31, 2022 (Pending Budgetary Approval).

Finding 7.

Condition: District 3 Data Center Flood Risk:

- There is no leak detection system for the data center.
- Radio Shop Data Center Flood Risk:
- There are no raised floors.
- There is no floor drain in the data center.
- There is no leak detection system for the data center

Recommendation 7: Enhance flood prevention controls including:

Installing floor drains, leak detection systems, and raised floors or other compensating controls.

Response: The Milwaukee Police Department is making this a part of their long term strategic plan with an implementation date of December 31, 2025 (Pending Budgetary Approval).

Finding 8.

Condition: The Radio Shop location is a raised space inside a garage approximately 1 story off the ground. There are windows on the exterior walls of the space.

Recommendation 8: Eliminate all windows on exterior walls.

Response: The Milwaukee Police Department is making this a part of their long term strategic plan. The Milwaukee Police Department plans to have this finding remediated by December 31, 2026 (Pending Budgetary Approval).

Finding 9.

Condition: MFD Policies & Procedures are seriously deficient as follows:

- Of the 8 general policies recommended by Best Practices, MFD has not developed 6 (75%) of them.
- The missing P&P are: Access control, Data Security, Physical Security, Environmental Standards, IT Inventory and Vendor Management, and Data Center Capacity and Upkeep Management. (This should not be considered an all-inclusive list of best practice P&P, but rather, a representative minimum.)
- Of the P&P that exist, there is no evidence of periodic review and update, and no evidence they have been updated since 2011.
- MFD has some general policy, but is lacking in detailed procedures implementing the policies.

MFD shares data center facilities with the Milwaukee Police Department (MPD) and often defers to MPD for P&P. However, MFD cannot produce the MPD P&P to which they defer.

Recommendation 9: MFD should develop its own set of data center policies and procedures specifically for MFD, independent of MPD, including the following:

- Develop policy for the items recommended by Best Practices;
- Implement a formal periodic review process that includes evidencing review and updates with management signature and date.
- Store all policies and procedures in a centralized, easily accessible location to facilitate accessibility and departmental cohesion.
- Develop detailed procedures implementing department policies.

Response: Both the Milwaukee Fire Department and the Milwaukee Police Department are working on their policies and procedures as a part of their long term strategic plans. Policies and Procedures will be updated by December 31, 2021.

Finding 10.

Condition: The District 3 Data Center access list contains 101 individuals. Based on the testing of physical access, 4 (4% of total) individuals had access privileges that were no longer needed.

The Radio Shop access list contains 83 individuals. Based on the testing of physical access, 3 (or 3.6%) of the individuals had access privileges that were no longer needed. These same individuals were also on the District 3 Data Center access list.

Recommendation 10: Perform and document periodic physical-access reviews

To strengthen processes and controls surrounding physical access to the District 3 and Radio Shop data centers, management should:

1. Perform periodic, formal physical access reviews for all individuals with access to Fire Department server rooms for appropriate access levels, including the removal of access for employees separated from City service or transferred to areas that do not require access. Police Department should have the final approval regarding all access decisions with input from Fire Department regarding Fire Department personnel. This review should be performed in addition to, and perhaps simultaneously with, the review that is done of non-MPD department members to MPD facilities.

Retain the documentation evidencing the completion of the periodic review, any changes made because of the review, and management approval evidenced by signature and date.

Response: Access controls for the District 3 Data Center and the Radio Shop are managed by the Milwaukee Police Department. They are working on remediating this finding and have an expected remediation date of December 31, 2020 (Pending Budgetary Approval).

Finding 11.

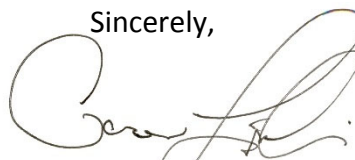
Condition: Visitor sign in logs are not maintained at either data center location.

Recommendation 11: Establish policy and procedure requiring the use of visitor logs at both data center locations which requires:

- All visitors to sign the log and provide proper identification;
All visitors to be escorted by a responsible employee.

Response: The Milwaukee Police Department is responsible for monitoring visitor logs for the District 3 Data Center. This finding has been remediated.

Sincerely,



AARON LIPSKI
Assistant Chief
Support Bureau

AL/JM/cf

Martin Matson
Comptroller

Aycha Sawa, CPA, CIA
Deputy Comptroller



Toni Biscobing
Special Deputy Comptroller

Rocklan Wruck, CPA
Special Deputy Comptroller

Office of the Comptroller

November 13, 2019

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 the Milwaukee Fire Department 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,

A handwritten signature in black ink that reads "Martin Matson".

Martin Matson,
Comptroller