Audit of Badge Access (DPW-Controlled)

AYCHA SAWA
City Comptroller

CHARLES ROEDEL
Audit Manager

City of Milwaukee, Wisconsin

August 2021

Table of Contents

Aycha Sawa, CPA, CIA
Comptroller

Joshua Benson
Deputy Comptroller

Toni Biscobing
Special Deputy Comptroller

Richard Bare, CPA
Special Deputy Comptroller

August 13, 2021

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

Dear Mayor and Council Members:

The attached report summarizes the results of the Audit of Badge Access (DPW-Controlled). Specifically included in the scope were:

- All individuals with current access to DPW-controlled spaces.
- Transferred employees between departments within the period HRMS data is available.

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

- Determine if terminated employees and other individuals who should not have badge access do not have badge access.
- Determine if transferred employees between departments within the period HRMS data is available have had badge access to their former departments removed.
- Assess the root cause of process deficiencies for departments with significant badge access issues identified.

The audit identified control design improvement opportunities to reduce inappropriate and unnecessary access, as well as opportunities to communicate responsibilities to departmental managers to improve their understanding. 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 Department of Public Works.

Sincerely,

Charles Roedel

Charles Roedel, CPA, CIA
Audit Manager

CRR:ny

Audit Report Highlights

Audit of Badge Access (DPW-Controlled)

Why We Did This Audit

Government offices can be targets for theft, unlawful entry, kidnapping, bombings, forcible occupation, and sabotage. Effective barriers, both physical and psychological, can reduce the likelihood of these threats. These barriers can be created through effective security management.

Objectives

The objectives of the audit were to assess whether badge access controls were in place and operating effectively to limit access to people who should have access in spaces where they should have access.

Background

The City of Milwaukee uses badges to obtain access to various areas of the City. Security management is the process of identifying, implementing, and monitoring systems and processes for the protection of people and building assets against loss, misuse, damage, or deprivation of use caused by deliberate acts. It is imperative that badge access is removed from people no longer working at the City. If a person transfers between departments, the badge should be reviewed for appropriate access with removal or additions made as necessary.

Five departments control badge access at the City: MPD, MFD, MPL, ERS and the DPW. DPW controls access for all departments other than MPD, MFD, MPL, and ERS.

Overview

Opportunities exist to reduce inappropriate and unnecessary badge access to DPW-controlled spaces. Personnel responsible for badge access management are relatively new to their roles and have made demonstrable progress. However, there remain significant opportunities for a more understood, thorough, systematic, and sustainable process.

Opportunities for Improvement

Department Head Access Reviews: The access of former employees is not always terminated timely. Additionally, employee ID numbers are not consistently entered and employee departments are often outdated in the badge access system.

Departmental Manager Guidance: There is no comprehensive document to provide to departmental managers under the DPW badge access umbrella with guidance on their role in badge access creation, access changes, information changes (e.g., name changes), reactivation, and return.

Policies and Procedures: Internal (i.e., DPW badge access group) policies and procedures do not exist for badge processes.

Clearance Space Access Reviews: Badge clearances do not have owners identified or descriptions of what they are protecting.

Inactivity Deactivation Setup: Inactivity deactivations are not consistently set up in the badge access system.

(Recommendations can be found in the Audit Conclusions and Recommendations section of this report.)

I. Audit Scope, Objectives, and Methodology

Scope

The scope included DPW-controlled badge access. Specifically included in the scope are:

- All individuals with current access to DPW-controlled spaces.
- Transferred employees between departments within the period HRMS data is available.

Specific exclusions from scope were:

- MPD, MFD, ERS, and Library-controlled badge access.
- Transferred employees between departments prior to the period of HRMS data availability.
- Access within departments.

Objectives

The objectives of the audit were as follows:

- Determine if terminated employees and other individuals who should not have badge access do not have badge access.
- Determine if transferred employees between departments within the period HRMS data is available have had badge access to their former departments removed.
- Assess the root cause of process deficiencies for departments with significant badge access issues identified.

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 badge access. The audit program was developed using criteria outlined by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), Control Objectives for Information Technologies (COBIT), Federal Information System Controls Audit Manual (FISCAM), and National Institute of Standards and Technology (NIST). These present a methodology for performing audits 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 procedures developed to evaluate the processes and controls to meet the audit objectives included process walkthroughs, 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 DPW badge controlled areas based on HRMS active employee list and DPW badge application list based on the principle of least privilege[1].

II. Organization and Fiscal Impact

The City of Milwaukee uses identification badges to obtain access to various areas of the City. Security management is the process of identifying, implementing, and monitoring systems and processes for the protection of people and building assets against loss, misuse, damage, or deprivation of use caused by deliberate acts. It is imperative that badge access is removed from people no longer working at the City. If a person transfers between departments or has a change in responsibilities, their badge should be reviewed for appropriate access with removal or additions made as necessary.

Five departments control badge access at the City: Milwaukee Police Department (MPD), Milwaukee Fire Department (MFD), the Library, Employes' Retirement System (ERS), and the Department of Public Works (DPW). The Department of Public Works controls access for all departments other than MPD, MFD, ERS, and the Library.

III. Audit Conclusions and Recommendations

Opportunities exist to reduce inappropriate and unnecessary badge access to DPW-controlled spaces. Personnel responsible for badge access management are relatively new to their roles and have made

[1] Federal Information Systems Controls Audit Manual (FISCAM), GAO IT Manual, AC-6.4.4, p. 266

demonstrable progress. However, there remain significant opportunities for a more understood, thorough, systematic, and sustainable process.

Department Head Access Reviews

In a best practice control design, management would conduct regular reviews of individuals with physical access to sensitive areas to ensure such access is appropriate.[2] DPW badge access management was able to demonstrate significant progress in eliminating unnecessary access during the course of the audit. However, an opportunity exists to develop a thorough, systematic, and sustainable process to regularly review access.

Finding: The access of former employees is not always terminated timely. Additionally, employee ID numbers are not consistently entered and employee departments are often outdated in the badge access system.

Risk: Individuals could gain access to a space to which they should not have access. *Risk Rating: High*

Recommendation 1: Send badge access lists to department heads at least annually and require the department heads confirm whether the employee is an active employee within their department and enter any incomplete information. Utilize updated lists for more efficient termination audits.

Departmental Manager Guidance

Without a well-designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, or improperly implemented; and controls may be inconsistently applied[3].

Finding: There is no comprehensive document to provide to departmental managers under the DPW badge access umbrella with guidance on their role in badge access creation, access changes, information changes (e.g., name changes), reactivation, and return.

[2] Federal Information Systems Controls Audit Manual (FISCAM), GAO IT Manual, AC-6.4.4, p. 266
[3] NIST 800-53, PS-1, Personnel Security Policy and Procedures, Appendix F-PS, p. F-145

Risk: Inconsistent execution of creation, access changes, information changes (e.g., name changes), reactivation, and return of badges due to lack of understanding of the process by management of the departments under the DPW badge access umbrella. *Risk Rating: Medium*

Recommendation 2: Create and distribute comprehensive guidance to provide to managers under the DPW badge access umbrella regarding their responsibilities for creation, access changes, information changes (e.g., name changes), reactivation, and return of badges. The guidance should be reviewed by DPW badge access management at least annually.

Policies and Procedures

Without a well-designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, or improperly implemented; and controls may be inconsistently applied[4].

Finding: Internal (i.e., DPW badge access group) policies and procedures do not exist for badge processes.

Risk: Lack of policies and procedures could result in inconsistent execution of responsibilities. *Risk Rating: Low*

Recommendation 3: Document internal policies and procedures for badge creation, access changes, information changes (e.g., name changes), deactivation, reactivation, retrieval, redeployment, and disposal. Policies and procedures should be reviewed annually and signed as evidence of review.

Clearance Space Access Reviews

The DPW badge access team groups individual clearances into clearance groups. A clearance could be for a particular door and a clearance group would be a grouping of clearances that would be associated together (i.e., expected clearances for a particular department). In a best practice control design, management would conduct regular reviews of ownership of badge clearances to ensure such access is appropriate[5]. Employees transferring between departments or having their role change have the possibility of unneeded access if clearance groups are not reviewed. DPW badge access

[4] NIST 800-53, PS-1, Physical and Environmental Protection Policy and Procedures, Appendix F-PS, p. F-127
[5] Federal Information Systems Controls Audit Manual (FISCAM), GAO IT Manual, AC-6.4.4, p. 266

management has started to conduct clearances reviews. There is an opportunity to conduct reviews for all clearance groups.

Finding: Badge clearances do not have owners identified or descriptions of what they are protecting.

Risk: Access to clearance spaces may be inappropriate. *Risk Rating: Low*

Recommendation 4: Identify owners for each clearance group and have the owners review the access list for appropriateness at least annually. Fill in the badge system with notes about what the clearance is protecting.

Inactivity Deactivation Setup

The system used to control badge access, C-Cure 9000, allows for setup for badges to deactivate after a period of inactivity.

Finding: Inactivity deactivations are not consistently set up in the badge access system.

Risk: Unused cards can be found and used by unauthorized people. *Risk Rating: Low*

Recommendation 5: Inactivity deactivations should be consistently set up in the badge access system.

Aycha Sawa, CPA, CIA
Comptroller

Joshua Benson
Deputy Comptroller

Toni Biscobing
Special Deputy Comptroller

Richard Bare, CPA
Special Deputy Comptroller

August 25, 2021

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

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 Badge Access (DPW-Controlled). 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,

Aycha Sawa, CPA, CIA
Comptroller

Jeffrey S. Polenske, P.E.
Commissioner of Public Works
Jerrel Kruschke
City Engineer
Timothy J. Thur, P.E.
Infrastructure Administration Manager

City of Milwaukee

Department of Public Works
Infrastructure Services Division

August 10, 2021

Charles Roedel
Audit Manager
Comptroller's Office
200 E. Wells, Room 404

Subject: Audit of Badge Access (DPW – Controlled)

Dear Mr. Roedel:

In reply to your draft audit report received July 29, 2021, we offer the following response to your findings.

Department Head Access Reviews:
DER is providing a list of active and recently separated employees to DPW - Bridges and Buildings security staff on a monthly basis beginning July 2021. DPW security staff reconciles this list against the CCURE 9000 database as a monthly audit of active employees. Additionally, starting November 2021, DPW - Bridges and Buildings will be sharing with department heads a list of employees and their clearances, so that managers can confirm active employees and their clearances.

Departmental Manager Guidance:
ID Badge policy was updated July 21, 2021 and emailed to City of Milwaukee department heads and managers. This policy will be reviewed annually and updated as necessary. Review is scheduled for July 19, 2022.

Policies and Procedures:
Standard operating procedure is in the process of being written with completion expected by the end of September 2021.

Clearance Space Access Reviews:
Security team is in the process of identifying owners and setting up a policy for managers to review the access list annually. This project is expected to be completed by the end October 2021.

Inactivity Deactivation Setup:
Security team has setup a query to identify any user in the database that has no activity for three months. Security team will verify the employment status of individuals that appear on the query and respond as appropriate.

We appreciate your assist during the audit process to work toward making the necessary improvements to our process and ultimately to the security of our properties. If you have any further questions concerning this matter, please contact me, at (414) 286-3295 or ttarko@milwaukee.gov.

Sincerely,

Thomas E. Tarkowski
Engineer in Charge
DPW- Bridges and Buildings

C: A. Abubaker
J. Kruschke