Audit of Citizen Relationship Management (CRM) Application Controls

MARTIN MATSON
City Comptroller

ADAM FIGON
Audit Manager

City of Milwaukee, Wisconsin

February 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

February 6, 2018

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

Dear Mayor and Council Members:

The attached report summarizes the results for the audit of the Citizen Relationship Management (CRM) application controls. The scope of the audit included the CRM application and general controls. The audit objectives were as follows:

1. To assess the adequacy and effectiveness of the application and general controls supporting the CRM system and whether they are in compliance with applicable policies, procedures, and best-practice criteria;

2. To assess the adequacy and effectiveness of input, processing, output, and monitoring controls over the key-performance metrics of the Unified Call Center (UCC);

3. To determine the adequacy of data and security-administration controls and whether they have been implemented effectively; and

4. To verify the establishment of a business-continuity plan for the CRM application(s) and the UCC's operations.

The audit concluded that the application controls in place over the CRM are adequately designed and are operating effectively. The audit procedures demonstrated that information technology controls are adequate to ensure that business objectives are met and that appropriate best practice methods are utilized. However, enhancements are needed in the control design and operational effectiveness of the general controls. The audit report includes two recommendations to further improve the controls over the CRM application.

It is noted that departmental management proactively initiated mitigating actions deemed necessary to address some of the issues encountered, during the performance of the audit.

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 UCC and Information Technology and Management Division.

Sincerely,

Adam Figon

Adam Figon, MBA, CRMA
Audit Manager

ACF:gl

I. Audit Scope and Objectives

The audit examined the City's Unified Call Center (UCC) and encompassed policy and procedure, user access, change control management, security administration, application and general controls, performance metrics and business-continuity plans. Specifically, the scope of the audit covers the Information Technology (IT) controls over the Lagan Citizen Relationship Management (CRM) application module, which is technology created by the vendor KANA Software, Inc., a wholly-owned subsidiary of Verint Systems, as of 2014. The audit period was November 2015 through November 2017.

The audit objectives were as follows:

1. To assess the adequacy and effectiveness of the application and general controls supporting the CRM system and whether they are in compliance with applicable policies, procedures, and best-practice criteria;
2. To assess the adequacy and effectiveness of input, processing, output, and monitoring controls over the key-performance metrics of the UCC;
3. To determine the adequacy of data and security-administration controls and whether they have been implemented effectively; and
4. To verify the establishment of a business-continuity plan that is relevant to the CRM application and the UCC's operations.

The audit excluded system backup controls and system vulnerability considerations, as they will be tested during two other audits currently in progress. The audit also omitted activities performed by the Information Technology and Management Division (ITMD) not directly related to the UCC's activities.

The audit was conducted in accordance with generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence that provides 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 CRM application. To establish appropriate evaluation criteria for this audit controls and procedures specific to the CRM application, and the UCC, were compared to a best practice based controls-testing program. This program was developed by using the Information Systems Audit and Control Association (ISACA) best-practice criteria. ISACA 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,[1] FISCAM,[2] NIST SP 800-14,[3] and NIST SP 800-53, Revision 4.[4] These standards were relevant during audit testing, finding identification, and recommendation development.

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

- Review of internal policies, procedures, guidelines, and system information;
- Verification of the performance metrics reported to management;
- Compliance assessment with the City Password Policy;
- Review of system user access, and physical access to the UCC via employee card keys, based on the principle of least privilege;
- Adequacy assessment of user-access change control management, authorization, and monitoring;

[1] Control Objectives for Information and Related Technology (COBIT), created and managed by the independent, nonprofit ISACA (formerly known as the Information Systems Audit and Control Association and now only known by its acronym).

[2] *Federal Information Systems Controls Audit Manual (FISCAM)*. US Government Accountability Office, 2009.

[3] National Institute of Standards and Technology (an agency of the U.S. Commerce Department's Technology Administration) Special Publication (NIST SP), published in September 1996.

[4] Developed by the federal government's *Joint Task Force Transformation Initiative* Interagency Working Group and published by NIST in April 2013.

- Verification that application change control management demonstrates appropriate authorization, approval, testing, and implementation;
- Verification that a contingency plan exists for high-call volume periods; and
- Evaluation of the business continuity plans to recover from system outages.

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 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 to lead the City in using and sharing information via ways that will provide the maximum efficiency and greatest benefit to Milwaukee citizens, businesses, and City government.

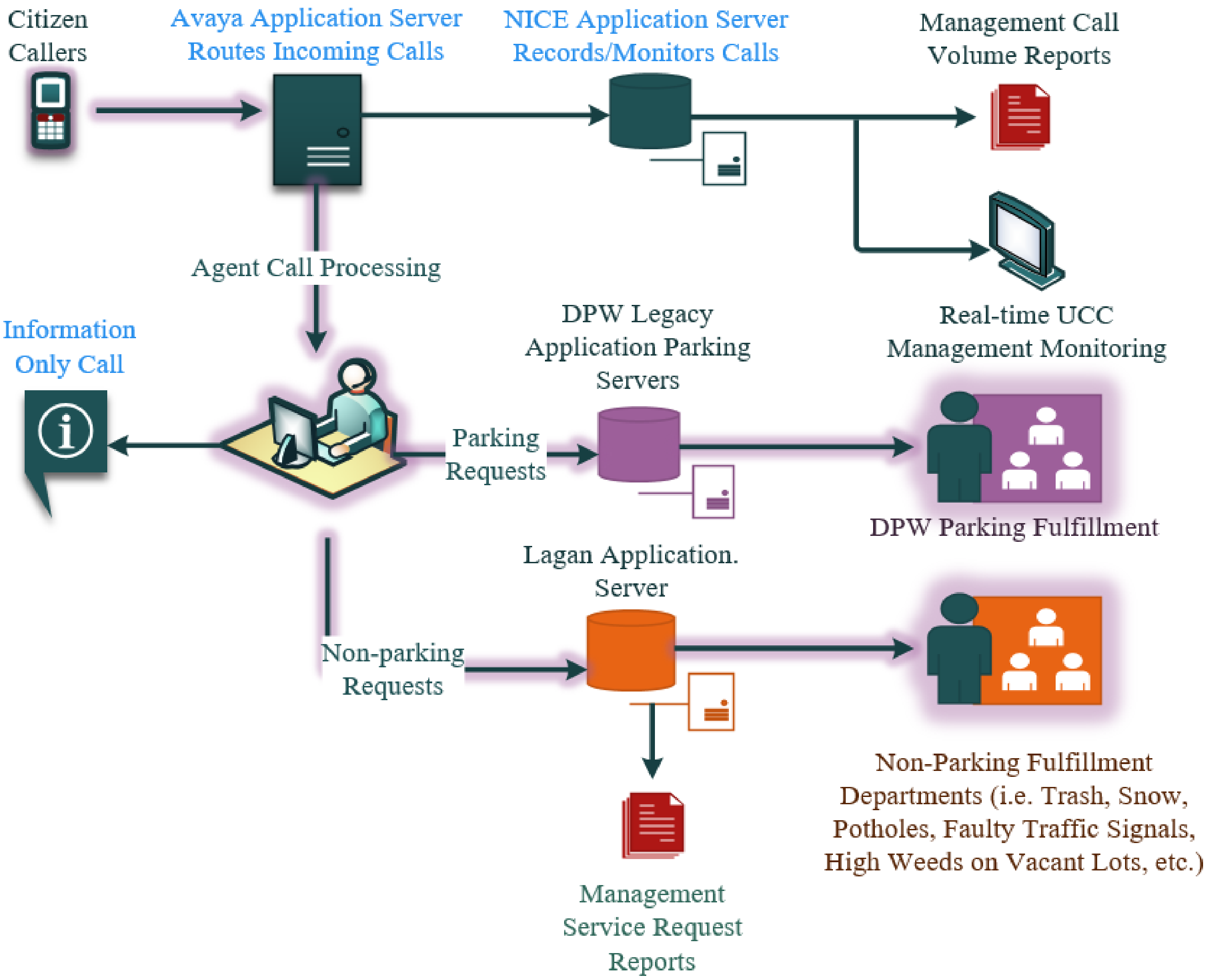
UCC Mission

The UCC's mission is to provide the public with quick access to all of Milwaukee's city services and essential information through multiple channels. The UCC strives for the highest possible level of customer service. The UCC helps agencies improve service delivery by allowing them to focus on their core missions and manage field-level work more efficiently. For many citizens, their only periodic contact with the City is through the UCC; thus, it is critical that citizens receive timely and accurate information and/or fulfillment of their service requests.

UCC Scope of Activity

The UCC processes a wide range of citizen concerns, such as patching potholes, removing abandoned vehicles and graffiti, trimming uncut grass, eliminating curbside trash, and the repair of faulty traffic signals. The UCC fields calls for Milwaukee's various departments, including Neighborhood Services, Public Works, City Development, Parking, and the Election Commission. Each time a service request is completed, the citizen is assigned a tracking number that can be used to determine when a City representative expects to investigate or resolve the request. Figure 1, below, represents the UCC call workflow process.

Figure 1
UCC Call Work Flow Process



Citizen Callers
Avaya Application Server Routes Incoming Calls
NICE Application Server Records/Monitors Calls
Management Call Volume Reports
Agent Call Processing
Real-time UCC Management Monitoring
Information Only Call
DPW Legacy Application Parking Servers
Parking Requests
DPW Parking Fulfillment
Lagan Application. Server
Non-parking Requests
Non-Parking Fulfillment Departments (i.e. Trash, Snow, Potholes, Faulty Traffic Signals, High Weeds on Vacant Lots, etc.)
Management Service Request Reports

UCC Fundamentals

The Lagan CRM system is the customer management system used by the UCC and is administered and maintained by the ITMD, with the application servers housed onsite at the ITMD. The UCC is a centralized office, staffed by City employees and located in the Zeidler Municipal Building. It is used for receiving and transmitting a large volume of citizen questions and service requests, through the use of telephones and computers, and provides the means of managing citizen interactions. The UCC's open workspace houses both supervisor stations and agent workstations, equipped with a computer and a telephone set/headset. The UCC's telecom switch can be independently operated or networked with additional, remote City personnel during periods of high-call volume, such as severe winter storms or election years. All call agents can view a large screen that enables monitoring of the number of citizen calls waiting in a queue and callers' wait time. In summary, call agents use CRM to receive, process, submit service-request work orders, and monitor the disposition of information and service requests through the UCC and its online service-request systems, email, and the MKE Mobile application.[5]

UCC Processing

On average, the UCC processes approximately 1,500 citizen interactions (calls, Click4Action service requests, MKE Mobile service requests, elected official service requests, and emails) per business day, with a lower volume during the weekends. The UCC handles more than 90% of parking information, permission, and complaint calls. In the first half of 2017, service and information requests from "Click for Action" and other web channels accounted for 27% of total citizen interactions. The area provides assistance to the Election Commission during local and national elections by receiving overflow calls. The Call Center is open seven days a week and employs eleven full-time City employees and a fluctuating number of temporary employees, with business hours that run from 7:00 a.m. to 1:00 a.m. Mondays through Fridays, 8:00 a.m. to 4:45 p.m. Saturdays, and 8:00 a.m. to midnight Sundays. The late night weekday hours accommodate citizen overnight parking needs, and the weekend hours accommodate citizen parking enforcement requests and Sunday night overnight parking requests.

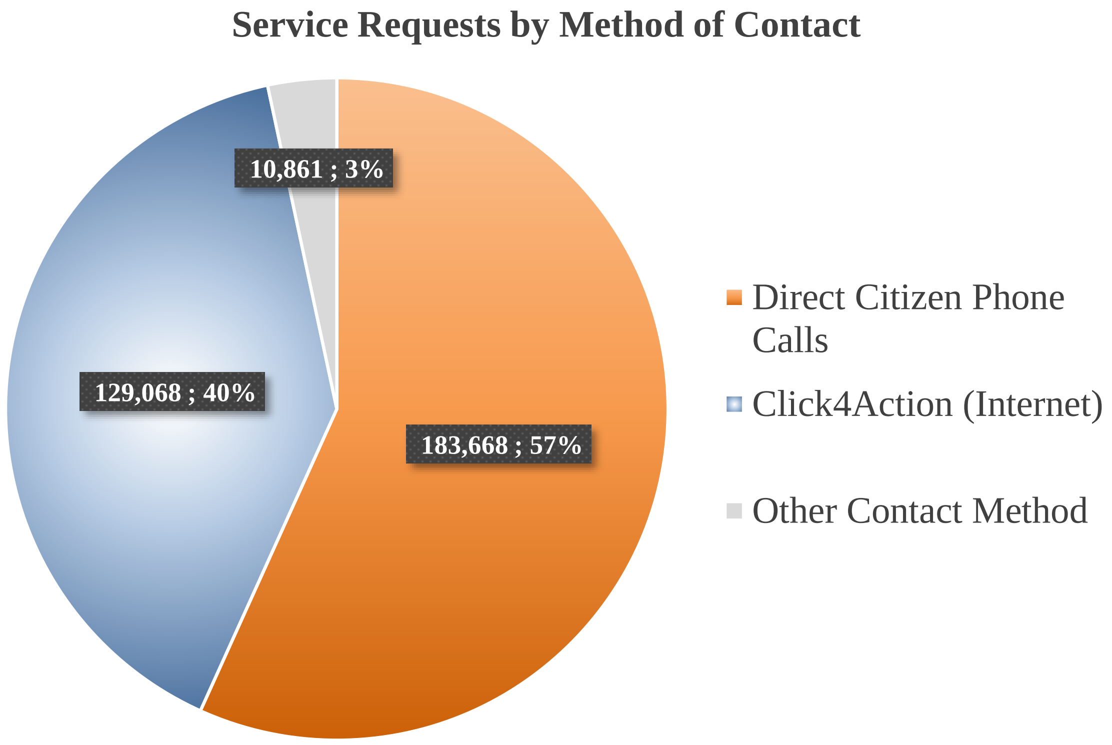
[5] A free smartphone application that provides Milwaukee residents a means to file UCC-service requests directly from a mobile telephone (available at App Store or Google Play).

2016 UCC Citizen Contact Volume and Statistics

The table and chart below present notable information about UCC operations.

Phone Call Statistics[6]	
Percentage of Calls Answered	95.4%
Call Abandonment Rate	4.6%
Average Actual Call Answer Time (2015)	33 seconds

Other Citizen Interactions	
Direct Citizen Calls Serviced	183,668
Click4Action (Internet) Service Requests	129,068
Emailed Service Requests	3,802
Aldermanic Service Requests	3,398
Mayor Office Service Requests	1,883
MKE Mobile App Service Requests	1,776
Mail Service Requests	2
Total Citizen Interactions	**323,597**



[6] *2017 Executive Budget Review*, page 5.

III. Audit Conclusions and Recommendations

UCC Operations–Key Control Elements

To be reliable and effective the CRM application, and related supporting applications, should demonstrate the following key elements of a control, based on best practice:

- **Data Confidentiality:** Appropriate controls should be in place to authorize and authenticate users, based on job responsibilities and the least-privilege access principle, while complying with City Password Policy criteria.

- **Data Integrity:** Appropriate controls should be in place to ensure the accuracy of the system's input, processing and reporting results, and application change management.

- **Data Availability:** Appropriate controls should be in place to provide easy access to data, wherever and whenever needed, thus helping to minimize or eliminate system downtime and business disruption events that can lead to lost productivity and service interruptions affecting citizens.

Application and General Controls

For information systems, the two main types of control activities are application and general controls. Application controls include the software's internally-programmed controls over data input, processing, and output that provide assurance to management that all CRM questions and service requests are received in a timely manner and accurately recorded. General controls include logical and physical security, access and change management, separation of duties, contingency planning, and business-continuity planning. The audit assessed the adequacy and effectiveness of the application and general controls in place that promote efficient and effective CRM application call input, storage, output, and dispatch of services.

The audit concluded that the application controls in place over the CRM are adequately designed and are operating effectively. The audit procedures demonstrated that information technology controls are adequate to ensure that business objectives are met and that appropriate best practice methods are utilized. However, enhancements are needed in the control design and operational effectiveness of the general controls. The audit report includes two recommendations to further improve the controls over the CRM application.

1. Document and retain periodic application-access reviews.
2. Document and retain periodic physical-access reviews.

Additional details regarding the recommendations for enhancement are provided in the following sections of this report. Lastly, a sample of performance metrics was tested for effectiveness of input, processing, output, and monitoring controls. No exceptions were noted.

A. Application Access and Change Control Management

According to best-practice requirements, including the *2013 COSO Framework–Principle 11*, management should select and develop general control activities over technology to support the achievement of objectives and respond to risks. Points of focus are as follows:

- ➢ Management should establish relevant security-management processes that are designed and implemented to restrict technology-access rights to authorized users commensurate with their job responsibilities.

- ➢ By preventing unauthorized system use and changes, data and program integrity are protected from malicious intent (e.g., someone gaining unauthorized access to the technology).

User-Access Monitoring and Maintenance

In accordance with best practice, applications should undergo periodic user-access and user-account reviews. User access should be granted using least-privilege criteria, based on job responsibilities, and approved by an authorized resource owner. Access should be disabled on a timely basis for terminated or transferring personnel while user access changes should be tracked, monitored, and documented.

The UCC maintains access to the CRM system through use of the Active Directory (AD) single sign-on process. All groups are created, maintained, and assigned through use of Active Directory. Upon login to any workstation, a user's login credentials are automatically routed to the CRM system for access. The password policy at the UCC conforms to those established by City guidelines. The UCC also manages various user groups and assigns the appropriate level of user access based on least-privilege criteria. Upon notification of an employee's separation from the City by management, both the employee's CRM system access and workstation AD access are removed. ITMD also monitors the Human Resources Management System (HRMS) for separated employees and verifies that their system access (within AD and email) has been removed.

Based on audit testing, it was determined that a number of users had unauthorized access to the CRM application and periodic user-access reviews were not being performed. With regard to change control management testing, no exceptions were noted.

Recommendation 1: Document and retain periodic application-access reviews.

To strengthen processes and controls surrounding physical access to the UCC, management should:

1. Perform a periodic, formal user-access review for all individuals with access to the CRM for appropriate access levels, including the removal of access for employees separated from City service or transferred to areas that do not require UCC access.
2. Eliminate generic IDs that are identified in the review.
3. Retain the documentation evidencing the completion of these periodic reviews, any changes made as a result of the reviews, and all management review-related actions.

B. Physical Access to the Unified Call Center

Physical Access

Adequate physical security controls should be established that mitigate the risks of physical damage, unauthorized access or the risk of harm to employees. 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 including contractors and other third parties. In addition, procedures should be implemented to terminate access privileges for terminated or separated employees or contractors.[7]

In conjunction with ITMD management approval, the Department of Public Works' Operations and Maintenance Manager establishes physical access to the UCC by assigning electronic key-card access to the room for all UCC personnel and other authorized employees (i.e., custodial workers and certain ITMD employees). An access-permission record of all employees having access to the UCC was provided to Internal Audit and tested for least-privilege access. Based on audit testing, it was determined that the number of employees with physical access to the UCC significantly exceeds the number of users needing UCC access for work purposes.

Recommendation 2: Document and retain periodic physical-access reviews.

To strengthen processes and controls surrounding physical access to the UCC, management should:

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

[7] *Federal Information Systems Controls Audit Manual (FISCAM)*. US Government Accountability Office, 2009, p. 260.

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.

C. Business-Continuity and Disaster-Recovery Planning

Business continuity encompasses planning and preparation to ensure that the UCC 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 CRM application and supporting applications 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.

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.

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

Business-Continuity Test, Training and Exercise Program

The audit included a review and evaluation of the CRM application, supporting applications, and business-continuity plans, necessary to recover from a system outage, based on industry best practices and guidelines established by ISACA.

One of the objectives for the audit was to verify the establishment of a business continuity plan (BCP) for the CRM. After review of the BCP it was determined that the UCC has some elements of a viable plan, however, the overall completeness of the plan (especially in the areas of testing, training, and simulation exercises), needs improvement. The challenge facing the UCC is not limited in scope to the UCC, but is representative of an overarching need for a complete BCP for the ITMD as a whole, of which, the UCC is only one important part. As such, the emphasis should be on an all-inclusive approach for the entire range of software applications under management of the ITMD. A BCP recommendation for the ITMD will be forthcoming in the *ITMD Data Center Controls Audit* which is currently underway and scheduled to be complete in the first quarter of 2018.

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

February 1, 2018

Adam Figon
Audit Manger
Office of the Comptroller
City Hall, Room 404

RE: Audit of Citizen Relationship Management (CRM) Application Controls

Dear Mr. Figon:
This is the Department of Administration's Information and Technology Management Division's written response to the two recommendations made in the *Audit of Citizen Relationship Management (CRM) Application Controls* dated February 2018.

Recommendation 1 – **Document and retain periodic application-access reviews.**
At no time was security compromised since access to the CRM application requires two levels of security. While the CRM login was active for some former employees, in all cases the Active Directory (AD) login for these users was deactivated at the time they left the UCC. In an effort to maintain good records, ITMD will perform semi-annual user-access reviews on the CRM application. Semi-annual reviews will be conducted in March and October 2018. The IT Security and Audit Analyst position will be responsible for conducting the review with the UCC Manager.

Recommendation 2 - **Document and retain periodic physical-access reviews.**
Current procedures are to notify DPW Building Security when changes in the staffing and access is needed to the Call Center. ITMD will begin requesting the Access List from DPW on a semi-annual basis in March and October and communicate desired corrections/changes back to the DPW. The IT Security and Audit Analyst position will be responsible for requesting, reviewing and submitting changes to DPW.

Sincerely,

Nancy A. Olson

Nancy A. Olson

Martin Matson
Comptroller

Aycha Sirvanci, CPA, CIA
Deputy Comptroller

Toni Biscobing
Special Deputy Comptroller

Rocklan Wruck, CPA
Special Deputy Comptroller

Office of the Comptroller

February 6, 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 the Citizen Relationship Management (CRM) Application Controls* dated February 2018. 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