Audit of 9-1-1 System Application Controls

MARTIN MATSON
City Comptroller

ADAM FIGON
Audit Manager

City of Milwaukee, Wisconsin

August 2017

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

August 29, 2017

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

Dear Mayor Barrett and Council Members:

The attached report summarizes the results of the audit of the 9-1-1 system application controls. The scope of the audit included the 9-1-1 system application and general controls from September 2015 to March 2017.

The primary objective of the audit was to evaluate whether the internal controls in place over the 9-1-1 system are adequately designed and operating effectively. Specific audit objectives are as follows:

1. Assess whether the IT general controls over physical security, configuration management and system access, including privileged user and vendor accounts, are in compliance with department policy and best practice criteria as outlined by the Information Systems Auditing and Control Association (ISACA);

2. Assess whether the IT application controls over input, processing, output and data integrity, including system security maintenance, are in compliance with departmental policy and best practice criteria as outlined by ISACA; and

3. Evaluate the record of IT system availability and business continuity plans to recover from a system outage based on industry best practice and guidelines established by ISACA.

The audit concluded that the internal controls in place over the 9-1-1 system are adequately designed and operating effectively. The audit procedures demonstrated that the 9-1-1 information technology controls are adequate to ensure that business objectives are met and that appropriate best practice methods are both effectively utilized and rigorously advocated by the Office of Police Information Systems.

With few noted exceptions, the audit report includes eight recommendations to further enhance the controls over the 9-1-1system.

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

It is noted that for certain controls identified within this report department management proactively initiated mitigating actions 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, which is followed by management's response.

Appreciation is expressed for the cooperation extended to the auditors by the personnel of the Office of Police Information Systems.

Sincerely,

Adam Figon

Adam Figon, MBA, CRMA
Audit Manager

ACF:gl

I. Audit Scope and Objectives

The audit examined the Milwaukee Police Department (MPD)–Office of Police Information Systems' 9-1-1 system application controls. Specifically, the scope of the audit covers the Information Technology (IT) general and application controls over the Computer Aided Dispatch (CAD) and the Records Management System (RMS) modules of the application vendor, TriTech, Inc. The audit focused on policy and procedure, user access, change control management, security administration, application controls, vendor oversight, and business continuity plans. The audit period was September 2015 through March 2017.

The primary objective of the audit was to evaluate whether the internal controls in place over the 9-1-1 system are adequately designed and operating effectively. Specific audit objectives are as follows:

1. Assess whether the IT general controls over physical security, configuration management, and system access, including privileged user and vendor accounts, are in compliance with department policy and best practice criteria as outlined by the Information Systems Auditing and Control Association (ISACA).
2. Assess whether the IT application controls over input, processing, output, and data integrity, including system security maintenance, are in compliance with departmental policy and best practice criteria as outlined by ISACA.
3. Evaluate the record of IT system availability and business continuity plans to recover from a system outage, based on industry best practices and guidelines established by ISACA.

The audit scope does not include the daily management activities of the Police Department, Fire Department and Emergency Medical Services, or the daily staff management activity of Dispatchers or Telecommunicators.

The audit was conducted in accordance with generally accepted government auditing standards. Those standards require that the audit 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 CAD and RMS applications. To establish appropriate evaluation criteria for this audit, controls and procedures specific to the CAD and RMS applications and the Office of Police Information Systems were compared to a best practice based controls testing program. This program was developed by using the Federal Information Systems Controls Audit Manual (FISCAM), which 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). This information was used as a reference for the planning and program development of this audit. The audit program and procedures also included elements from best practice criteria COBIT/ISACA, COSO, NIST SP 800-14, and NIST SP 800-53 (Revision 4).[1] These standards were relevant during audit testing, identification of findings, and development of recommendations.

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:

- Reviewed internal policies, procedures, guidelines and system information;
- Reviewed Call Center physical security;
- Assessed compliance with the City Password Policy;
- Reviewed system user access, based on the principle of least privilege;
- Reviewed the 9-1-1 computer room access, based on the principle of least privilege;
- Reviewed computer room environmental controls and physical security;

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

- Assessed the adequacy of user access change control management, authorization, and monitoring;
- Identified and reviewed key automated system edit controls;
- Assessed performance of the ongoing monitoring of the application risks and its third-party vendor, and reviewed vendor contract provisions;
- Examined data backup controls, processes, and documentation;
- Evaluated the record of IT system availability; and
- Evaluated the business continuity plans to recover from a system outage.

II. Organization and Fiscal Impact

The MPD vision is a Milwaukee where all can live safely and without fear, protected by a police department with the highest ethical and professional standards.[2] The MPD states their mission as, "In partnership with the community, we will create and maintain neighborhoods capable of sustaining civic life. We commit to reducing the levels of crime, fear, and disorder through community-based, problem-oriented, and data driven policing."[3]

Office of Police Information Systems

The Office of Police Information Systems (OPIS) is responsible for the planning and management of all information technology projects and the overall information environment with a current budget of approximately $3+ million within the Milwaukee Police Department. The OPIS also has responsibility to plan, develop, and implement major technology initiatives to improve the overall efficiency of the department and is responsible for future planning and budgeting for the modernization and upgrading of current systems in the rapidly changing environment of urban law enforcement. Lastly, the OPIS serves as liaison with Federal, State, and other municipal, public safety agencies, regarding technology collaboration and cooperation; and provides direct supervision of the Central Records Division, Communications Division, and Data Services Division.

[2] Milwaukee Police Department Annual Report 2015, Page 1.
[3] Ibid.

Emergency Communications

9-1-1 emergency calls originate from a citizen cell or landline telephone and are received at OPIS's Technical Communication Division's emergency call center. This facility processes the City's emergency requests for the Police, Fire, and Emergency Medical Services. In 2015 there were over 853,000 calls received by Technical Communications which resulted in 260,000 dispatched calls for service.[4]

Emergency System

Once a telecommunicator receives, evaluates, and confirms pertinent emergency call information, the data is inputted into the CAD system while also populating the RMS module. The integrated CAD and RMS system applications, developed and supported by TriTech, Inc., is a third-party, vendor software package that provides MPD with its 9-1-1 emergency-call input, storage, dispatch, and retrieval functionalities. This application is administered by OPIS and technical support is provided by TriTech, Inc.

Upon completion of the call-input process, the emergency information is transferred electronically to the Police Dispatch area, where dispatchers identify the emergency assets needed and order the necessary resources to the emergency site, via police radio.

Dell KACE System

Dell KACE is a software that specializes in computer processing for systems management of information technology equipment. The Dell KACE application is developed and designed to help IT personnel more efficiently provision, manage, secure, change and service network-connected devices such as CAD and RMS. Technical change requests (called job tickets) are opened sequentially on the system, for tracking purposes, from the initial change request, approval, implementation, testing and the final signoff of the change. The history of the change activity, including the identify of all processors involved, is recorded permanently in reverse chronological order on the job ticket, and available for future reference and audit trail purposes.

[4] Ibid,10.

Operational Accreditation

It is also noted that in 2015 MPD operations (including communications and related processes) received acclaim via the achievement of agency accreditation with the Wisconsin Law Enforcement Accreditation Group.[5]

III. Audit Conclusions and Recommendations

Emergency System – Key Control Elements

To be reliable and effective, the 9-1-1 (CAD and RMS) emergency application systems should demonstrate the following best practice-based key elements of a control:

- **Data Confidentiality-** appropriate controls should be in place to authorize and authenticate users, based on job responsibilities and the least-privilege access principle, and comply with City Password Policy criteria;
- **Data Integrity-**the accuracy of the system's input, processing and reporting results, and application change management; and
- **Data Availability-**the ability to access data easily, wherever and whenever needed, and most importantly 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, there are two main types of control activities: 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 9-1-1 telephone calls are received and recorded, accurately and timely. General controls include logical and physical access, security, and change control management, separation of duties, contingency planning, and business continuity management. The audit assessed the adequacy and effectiveness of the application and general controls in place that promote efficient and effective 9-1-1 emergency-call input, storage, dispatch, and retrieval functionality.

[5] Ibid., 16.

The audit concluded that the internal controls in place over the 9-1-1 system are adequately designed and operating effectively. The audit procedures demonstrated that the 9-1-1 information technology controls are adequate to ensure that business objectives are met and that appropriate best practice methods are both effectively utilized and rigorously advocated by the Office of Police Information Systems.

With few noted exceptions, the audit report includes eight recommendations to further enhance the controls over the 9-1-1system.

1. Document and retain periodic user access reviews.
2. Document and retain user access change control management activity.
3. Configure Inform RMS for compliance with City password policy.
4. Document and retain Dell KACE periodic user access reviews.
5. Document the change approver on the Dell KACE activity log.
6. Enhance the business continuity test, training and exercise program, documentation, and policy.
7. Designate and train a backup CAD administrator.
8. Obtain the system vendor's third party assurance report.

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

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:

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

- By preventing unauthorized use of, and changes to the system, data and program integrity are protected from malicious intent (e.g., someone breaking into 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; and user access changes should be tracked, monitored, and documented.

In the Office of Police Information Systems, periodic reviews are performed by management to ensure appropriate user access levels and user accounts. Audit testing results confirmed that the CAD, RMS, computer room and vendor access levels and user accounts were appropriate; however, the audit identified that supporting documentation demonstrating the performance of the periodic system access reviews, and any notable results or follow-up, is not being retained. Documentation was not available during the audit scope period from September 2015 to March 2017.

Additionally, audit procedures identified that one vendor training account was no longer needed (and was subsequently deactivated), and one user with access to the computer room had separated from City employment and required access deactivation.

Recommendation 1: Document and retain periodic user access reviews.

To strengthen access monitoring controls over the CAD and RMS applications, and the computer room, Management should:

1. Continue to perform and document the system user access and user account periodic reviews for all CAD, RMS and computer room users for appropriate access levels and permissions, terminations or transfers.
2. Retain the documentation evidencing the completion of periodic reviews, any changes made as a result of the reviews, and management approvals for the two most recent reviews.

This review only applies to the approximately 214 employees in Technical Communications Division and the 32 employees in the Technology Division of the MPD.

User Access Change Maintenance

In accordance with best practice requirements, maintenance of information systems should ensure that user access to these systems is appropriately restricted and that this user access change control management is tracked, monitored, and documented. User access changes must also be performed utilizing the standard concept of adequate separation of duties. This is intended to prevent errors and mitigate fraud risks by ensuring that no one individual monitors or reviews their own work or tasks. User access change controls help protect the integrity of the application data.

A standard operating procedure is utilized when a request to change (grant, revoke, or disable) a CAD, RMS, and computer room user's access is generated by the Office of Police Information Systems supervisory or management personnel. This procedure requires the use of the department's standard email access change form from Senior Management. The email indicates the stages of the process (request, approval, completion, and verification) and includes date confirmation of each stage. The retention of the user access change forms and the noted Management emails are recommended, per best practice, for all access changes.

Audit testing results indicated that the system user access change emails from Management, used to document the granting, revoking, or disabling of CAD, RMS, and computer room user accesses were not consistently retained during the audit period by the Office of Police Information Systems. Documents supporting the user access changes were not available.

Recommendation 2: Document and retain user access change control management activity.

To strengthen user access change control management over CAD, RMS, and the computer room, Management should utilize a standard and formal process that requires:

1. The retention of documentation for the timely granting, revoking, and disablement of all CAD, RMS, and computer room user access, which includes the user system access change forms and management approval emails, as applicable.
2. The separation of duties for access requests, approvals, performance of an access change, and final verifications of the changes.

This review only applies to the approximately 214 employees in Technical Communications Division and the 32 employees in the Technology Division of the MPD.

City Password Policy

The current TriTech RMS password configuration parameters are not capable of meeting City password policy in terms of password length, alphanumeric requirements, change frequency and the number of unsuccessful logon attempts. However, the latest version of TriTech Inform RMS is capable of maintaining compliance with City password policy. The new Inform RMS system is scheduled for conversion and live production in the second quarter of 2018.

Recommendation 3: Configure Inform RMS for compliance with City password policy.

To strengthen user access control over the Inform RMS system, Management should configure the new system password parameters to be compliant with City password requirements as a result of the scheduled 2018 system conversion.

Application Change Maintenance

In accordance with information system control standards, the maintenance controls over information systems and applications, or application change control management, should ensure that changes to an application are tracked, monitored, and documented; and were performed utilizing the standard concept of adequate separation of duties. Application change control management practices help protect the integrity of the application data by reducing errors.

Standard operating procedures have been developed and documented regarding CAD and RMS application-change controls. A standard Dell KACE application-change request form is used and is required to request CAD and RMS application changes. This application change request form indicates the stages of the process (request, completion, testing, and verification) and includes date confirmation of each stage. The retention of the Dell KACE application-change request form is required by Office of Police Information Systems management procedure and recommended per best practice, for all application changes.

Audit testing results indicated that a Dell KACE periodic access review was not performed recently or retained on file to demonstrate approval by a manager. Additionally, testing identified:

- Eight users that have separated from City employment and should have their access terminated;
- That all Dell KACE users have implicit change approval authority; and
- While all system changes are approved, a 'Change Approved By' field is not readily apparent on the Dell KACE activity log for each change request.

Recommendation 4: Document and retain Dell KACE periodic user access reviews.

Recommendation 5: Document the change approver on the Dell KACE activity log.

To strengthen the Dell KACE application change control management practices, Management should:

1. Perform a Dell KACE application user access review periodically and retain documentation of the results.
2. Perform access change updates as necessary.
3. Document change approver's name and the review date on the Dell KACE activity log.

B. Business Continuity Planning

Business continuity encompasses planning and preparation to ensure that the 9-1-1 Call Center continues to operate in case of serious incidents or disasters and is able to recover to an operational

state within a reasonably short period of time. As such, business continuity includes three key elements:

- **Resilience**–Critical business functions and the supporting infrastructure must be designed in such a way that they are materially unaffected by relevant disruptions. For example, through the use of redundancy and spare capacity;
- **Recovery**–Arrangements must be made to recover or restore critical and less-critical business functions that have failed; and
- **Contingency**–The 9-1-1 Call Center has a generalized capability and readiness to cope effectively with the occurrence of any major incidents and disasters. This includes those that could not have been foreseen. 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:

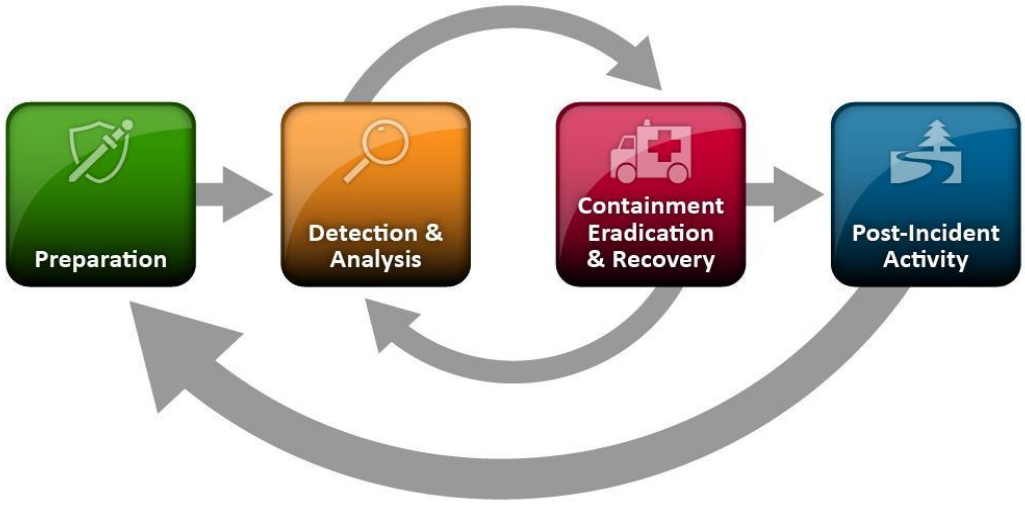
- **Preventive Measures**–Prevent an event from occurring;
- **Detective Measures**–Detect or discover unwanted events; and
- **Corrective Measures**–Correct or restore the system after an event occurs.

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 1 and emphasizes the incorporation of the feedback received through actual testing of the plan into improving the original disaster recovery plan.[6]

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

Figure 1
Overview of Business Continuity Framework



Business Continuity Testing

The audit included a review and evaluation of the 9-1-1 Call Center business continuity plans to recover from a system outage based on industry best practices and guidelines established by ISACA.

Test, Training, and Exercise Program

While the current Office of Police Information Systems business continuity test, training, and exercise (TTE) program is satisfactory, best practice and the standards required by ISACA and FISCAM necessitate enhancement of the TTE program. Specifically, this includes the following:

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

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

Recommendation 6: Enhance the business continuity test, training, and exercise program activity, documentation, and policy.

Management should enhance business continuity efforts through the following:

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

Testing the application contingency plan is essential to ensure it will function as intended when activated for an emergency.[7]

Backup CAD Administrator

The audit testing noted that a new backup CAD administrator should be formally designated and trained due to an employee retirement. Several current employees are available to perform the duties of the backup CAD administrator.

Recommendation 7: Designate and train a new CAD backup administrator.

To strengthen administrative and process controls over the CAD system, Management should formally designate and train a new backup CAD system administrator.

Third Party Assurance Report

Assurance reports are intended to meet the needs of a broad range of users that require detailed information and assurance regarding the control disposition of a user's software maintained or

[7] Federal Information Systems Controls Audit Manual (FISCAM), February 2009, Page 392.

developed at a third party service organization. The reporting covers relevant topics such as: security; system availability; processing integrity; and data confidentiality, privacy and integrity. The receipt and analysis of this reported information can play an important role in:

- Oversight of the organization and systems;
- Vendor management programs; and
- Internal corporate governance and risk management processes.

Analysis of a formal third party assurance report is not necessarily required, but it is considered a best practice for this emergency system. One alternative is for Management to perform an annual control/risk self -assessment which would include vendor management, ongoing viability of the vendor and processing integrity of the software. At the time of the audit, the third party software vendor TriTech did not yet complete a third party assurance report.

Recommendation 8: Obtain the system vendor's third party assurance report.

To strengthen business continuity control over the CAD and RMS systems, Management should obtain TriTech's third party assurance report. An alternative is for Management to perform an annual controls/risk self-assessment which would include vendor management, ongoing viability of the vendor and processing integrity of the software.

C. Application Controls

The objective of application controls are to ensure the completeness and accuracy of records and the validity of any entries made resulting from programmed processing activities.[8] The determination of the adequacy and effectiveness of the vendor developed and programmed CAD and RMS application controls configured to enforce appropriate business rules and controls over data inputs, processing, outputs, and reporting—was based upon the examination of relevant and correlated:

[8] Global Technology Audit Guide (GTAG) 8: Auditing Application Controls, 2009, Page 2.

- Testing of key input edit controls within CAD;
- Documentation reviews;
- Observations;
- Inspections; and
- Discussions with Management and personnel.

These procedures demonstrated that the vendor programmed application level controls, surrounding CAD and RMS, appear to be adequately designed to mitigate their related risks.

D. Computer Room Environmental Controls

The 9-1-1 Call Center computer room environmental controls encompass the practices and physical space in which the Call Center's computers, software, networking, and other equipment are maintained to support operations on a secure and uninterrupted basis. The hardware, data, applications, and servers are maintained in a secure, automated, and self-contained climate controlled environment. The determination of the adequacy and effectiveness of the computer room's environmental controls was based upon Internal Audit's physical observations, inspections, and testing. The environmental area controls reviewed during the audit (and select, relevant results) are as follows:

- Facility location (well mitigated flood and weather/storm risks);
- Facility and computer room access controls (two successive keycard entries are required with all entries logged)
- Climate controls (adequate regarding temperature, humidity, and sunlight);
- Fire suppression/detection systems and equipment (compliant with best practice):
- Adequate backup generator, generator testing and power surge protection; and
- An alternate Data Center processing facility is operational and available.

Internal Audit tested computer room user access for appropriateness, and one former employee was deactivated. These procedures demonstrated that the 9-1-1 Call Center computer-room

environmental controls appear to be adequately designed to mitigate their related risks and are consistent with industry best practices and guidelines established by ISACA.

E. Data Center Physical Security

Adequate physical security controls provide a safe and secure work environment and protect personnel, facility, and sensitive IT equipment that are all critical to accomplish the Department's mission. The audit included a review and evaluation of the physical security controls for the 911 Data Center and alternate data center processing facility. These environments are maintained on a 24/7 basis as the Data Center is staffed and operated continuously. The determination of the adequacy and effectiveness of the physical security control environment was based upon:

- Internal Audit's overall review of the facilities;
- Physical observations and inspections; and
- Comparisons to industry best practice and ISACA physical security criteria.

Data Center

The Data Center is housed in a modern building with a well-designed structure. The street level of the main processing site is constructed mostly of concrete and windowless, first floor walls. Building access is controlled by a system of keycard locks, and electronic records of all entry activity are maintained. Both the main Data Center and the alternate data center have multiple armed police officers on the premises to minimize the physical security risk and respond quickly to any incident that may arise. The physical area controls noted during the audit are as follows:

- The main IT facility and its computer operations, hardware and personnel appears to be of adequate size, and layout; and
- Facility security (MPD on site 24/7).

The procedures performed demonstrated that the 9-1-1 Data Center physical security controls appear to be adequately designed to mitigate their related risks and are consistent with industry best practices and guidelines established by ISACA.

Site, Power and Backup Contingencies

The alternate Data Center is located a distance from the main processing site that is considered reasonable under ISACA guidelines. Internal Audit tested one recent backup generator test for the main Data Center and one for the backup facility without exception.

Backup Testing

The Office of Police Information Systems has a process in place to continuously backup data and store it offsite in the event it is needed. The MPD 9-1-1 backup-tape process is automated and pre-programmed to run on a regular schedule and issue automated success or failure notifications to the system manager. The frequency of backups is consistent with ISACA guidelines. Internal Audit judgmentally selected a sample of backups for testing without exception.

BE A FORCE

Milwaukee Police Department
Police Administration Building
749 West State Street
Milwaukee, Wisconsin 53233
http://www.milwaukee.gov/police

Edward A. Flynn
Chief of Police

(414) 935-7200

August 25, 2017

Adam Figon, MBA, CRMA
Audit Manager
Comptroller's Office, Audit Section
City Hall, Room 404

RE: Response to the Audit of the Milwaukee Police Department IT 911 System Application Controls.

Thank you for your audit of the Milwaukee Police Department (MPD) – Office of Police Information Systems. MPD appreciates the opportunity to work with your staff and appreciates and values the audit's recommendations for improving MPD's 911 System Application Controls by the 911 Systems Application Controls Audit.

We have reviewed the audit and offer the following responses to its recommendations:

Recommendations 1: Document and retain periodic user access reviews.

MPD – Office of Police Information Systems (OPIS) shares the audit's concern about documenting and retaining periodic user access reviews. The Office of Police Information Systems has currently contracted an outside consultant to develop this SOP along with proper documentation of reviews which includes retention policies of such review documents. Documentation and implementation will be completed by November 30, 2017.

Status Date: August 25, 2017

Recommendations 2: Document and retain user access change control management activity.

MPD – Office of Police Information Systems (OPIS) shares the audit's concern about retaining user access change control management activity. The Office of Police Information Systems has currently contracted an outside consultant to develop this SOP along with proper documentation of reviews which includes retention policies of such review documents. Documentation and implementation will be completed by November 30, 2017.

BE A FORCE

Milwaukee Police Department
Police Administration Building
749 West State Street
Milwaukee, Wisconsin 53233
http://www.milwaukee.gov/police

Edward A. Flynn
Chief of Police

(414) 935-7200

Status Date: August 25, 2017

Recommendations 3: Configure Inform RMS for compliance with the City Password Policy.

MPD – Office of Police Information Systems (OPIS) shares the audit's concern about being compliant with the City of Milwaukee Password Policy since the current RMS System being used by MPD is not capable of instituting such a policy. The Office of Police Information Systems has currently contracted with TriTech for the procurement and implementation of their Inform RMS System which will go live in May of 2018. This will allow MPD to become compliant with the City of Milwaukee Password Policy.

Status Date: August 25, 2017

Recommendations 4: Document and retain Dell KACE periodic user access reviews.

MPD – Office of Police Information Systems (OPIS) shares the audit's concern about documenting and retaining Dell KACE periodic user access reviews. The Office of Police Information Systems has currently contracted an outside consultant to develop this SOP along with proper documentation of reviews which includes retention policies of such review documents. The 8 users that separated from MPD had their access removed on July 2, 2017. Documentation and implementation will be completed by November 30, 2017.

Status Date: August 25, 2017

Recommendations 5: Document the change approver on the Dell KACE activity log.

MPD – Office of Police Information Systems (OPIS) shares the audit's concern about documenting and retaining Dell KACE activity logs. The Office of Police Information Systems has currently contracted an outside consultant to develop this SOP along with proper documentation of reviews which includes retention policies of such review documents. The 8 users that separated from MPD had their access removed on July 2, 2017. Documentation and implementation will be completed by November 30, 2017.

Status Date: August 25, 2017

BE A FORCE

Milwaukee Police Department
Police Administration Building
749 West State Street
Milwaukee, Wisconsin 53233
http://www.milwaukee.gov/police

Edward A. Flynn
Chief of Police

(414) 935-7200

Recommendations 6: Enhance the business continuity test, training and exercise program, documentation, and policy.

MPD – Office of Police Information Systems (OPIS) shares the audit's concern about enhancing the business continuity test, training and exercise program documentation and policy. The Office of Police Information Systems has currently contracted an outside consultant to develop this SOP along with proper documentation to ensure document updates, walkthroughs with appropriate personnel along with documenting periodic training activity. Documentation and implementation of this policy will be completed by November 30, 2017. The Office of Police Information Systems (OPIS) will perform the recommended simulation recovery training that includes a walkthrough and simulation recovery training with all appropriate personnel and documentation of the periodic training activity.

Status Date: August 25, 2017

Recommendations 7: Designate and train a new backup CAD Administrator.

MPD – Office of Police Information Systems (OPIS) shares the audit's concern about designating and training a new backup CAD Administrator. The Office of Police Information Systems is currently working with MPD HR and DER to hire the FTE responsible for being trained as the backup CAD Administrator. This position has been open for 5 months with the hope of having this position filled by the end of February, 2018.

Status Date: August 25, 2017

Recommendations 8: Obtain the system vendor's third party assurance report.

MPD – Office of Police Information Systems (OPIS) shares the audit's concern about obtaining the CAD and RMS Vendor's assurance report. The Office of Police Information Systems is currently working with TriTech to produce these assurance reports for CAD and RMS. MPD is working to have this completed by the end of February, 2018.

Status Date: August 25, 2017

BE A FORCE

Milwaukee Police Department
Police Administration Building
749 West State Street
Milwaukee, Wisconsin 53233
http://www.milwaukee.gov/police

Edward A. Flynn
Chief of Police

(414) 935-7200

Sincerely,

Charles P. Burki
Milwaukee Police Department - IS Director