City of Memphis
Internal Audit Service Center

IT General Controls Review Report
Police Services Division
August 10, 2015

INTERNAL AUDIT TEAM

CITY AUDITOR

Leon Pattman, CIA, CISA, CRMA, CMFO

AUDIT TEAM

Brian Ford, CIA, CISA, CRMA
Debbie Banks, CFE, CICA, CMFO

Credential Key:

ACRONYM	DESIGNATION
CFE	Certified Fraud Examiner
CIA	Certified Internal Auditor
CICA	Certified Internal Controls Auditor
CISA	Certified Information Systems Auditor
CRMA	Certified in Risk Management Assurance
CMFO	Certified Municipal Finance Officer

TABLE OF CONTENTS

This page left blank intentionally.

City of Memphis
TENNESSEE

A C WHARTON, JR. - Mayor
JACK SAMMONS - Chief Administrative Officer
EXECUTIVE DIVISION
Internal Audit Service Center
LEON PATTMAN, CIA, CISA, CRMA, CMFO
City Auditor

August 10, 2015

Mr. Toney Armstrong, Director
Police Services Division
City of Memphis
201 Poplar Ave., Suite 1205
Memphis, Tennessee 38103

Dear Director Armstrong:

Auditors have completed our performance audit of general controls over Police Services Information Technology (IT). We really appreciate the patience and cooperation of you and your IT management team as we worked through several project delays due to higher priority audit projects. However, the findings and recommendations contained in this report should assist management in conducting a more reliable, effective and efficient IT environment.

The objective of the audit was to evaluate the adequacy and effectiveness of Police Services internal controls relative to control objectives that include reliability, availability, stability, and the integrity of the information technology supporting Police operations.

To accomplish our objective, we interviewed Police Services IT management and support staff, documented and evaluated processes, reviewed documentation, and conducted selective transaction testing of IT controls for the period January 1, 2013 to December 31, 2013. We utilized judgmental sampling during selective transaction testing based on perceived risks. Therefore the results should not be extrapolated across the whole test population. The scope of the audit was limited to the IT environment supported solely by the Memphis Police Department IT operations. The general controls components included in the scope for this audit were physical and logical security, applications development and maintenance, change management, disaster recovery and backup planning, and IT facilities environmental features. The scope did not include the City Information Systems Division. Auditors conducted an exit conference with your IT management team on March 4, 2015 to review and update the findings and make sure all the information was accurate and relevant.

We concluded that overall internal controls over Police Services IT operations are satisfactory with the stated control objectives with the exception of a fully implemented disaster recovery and backup plan. Auditors identified additional control deficiencies that represent viable

Room 536 • 125 North Main Street • Memphis, Tennessee 38103-2089 • (901) 636-6241

opportunities to provide stakeholders with greater assurance that IT will be better suited to continuously meet the stated control objectives. The specific details of the audit are located in the Objectives, Findings & Recommendations Section, but we have provided a high-level summary of the audit results below:

Internal Controls Strengths:

- The informal design for logical security which helps provide for data integrity was adequate to address password administration and identity management. Management stated that the Criminal Justice Information Systems (CJIS) is the governing policy for logical security.

- Physical security for IT facilities was adequate and working effectively to adequately safeguard IT resources. We observed access control to the building and additional access control to sensitive and restricted areas within the facility. Also, CJIS is the governing policies for physical security.

- There was an informal process to acquire/develop and implement the technology needed to support Police operations. Additionally, auditors noted that there was either staff or contracted maintenance support for the hardware and software. The City IS Division accommodated some of the hardware for Police network operations and inherently would maintain the equipment that was its responsibility. Therefore, auditors concluded that controls were adequate to provide for the availability and stability of Police IT support systems.

- The informal change management process was satisfactory to ensure system reliability and data integrity after changes were made to hardware and software. Essentially, Police IT operations follow a process to approve, validate, test, and implement changes made to hardware configuration and software updates and modifications.

Internal Controls Deficiencies:

Generally regarding performance audits, internal control deficiencies are due to lack of adequate design or full implementation of the control. Normally, a deficiency will not allow management and employees to prevent, detect, and correct impairments to operational efficiency, effectiveness, or compliance to established governance (laws, regulations, grants, contracts, policies, etc.). Auditors believe that correcting the following control deficiencies will strengthen controls effectiveness and/or improve control design:

- The Police IT disaster recovery and backup controls design lack the requirement for data to be backed up offsite daily as required in the City Manual.

- Although Police management stated that Police will fully participate in the City's IS Division disaster recovery plan, auditors found no documented, approved, tested and distributed plan.

- The IT control environment has a design deficiency because auditors did not find specific, written procedures to implement policies for logical and physical security, application development and maintenance, change management, disaster recovery and backup, environmental control, and monitoring compliance to established controls. In instances where CJIS is the governing policy and required specific procedures, auditors did not find specific procedures. The cornerstone of an effective, efficient, and adequate control environment is a written, comprehensive policy and procedures document. It provides for continuity of operations during staffing changes and continuous accountability for employee performance with respect to meeting the noted control objectives.

We would also like to commend Police IT management and staff for taking immediate actions to resolve some audit exceptions caused by some of the deficiencies noted. For example, auditors confirmed that management took the following actions to remediate some exceptions noted during the audit:

- disabled unnecessary generic (non-person) and former employee accounts to reduce the inadequate accountability for transactions and the likelihood of unauthorized access,

- adjusted domain password requirement to meet best practices to provide better system access control to applications,

- removed data center access accounts not uniquely accountable to an individual to help prevent unauthorized access to IT facilities, and

- implemented logging service software to track and monitor system activity to better prevent, detect and correct potential security breaches; as well as security configuration compliance.

Our overarching recommendations are for Police management to address the disaster recovery and backup plan deficiencies immediately and implement and train IT employees on comprehensive general controls policies and procedures, in addition to the CJIS policy.

This review was conducted in compliance with government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions. Our audit may not necessarily disclose all weaknesses related to internal controls. The following pages

provide the details of our findings and recommendations.

Our audit process provides management with the opportunity to submit a written response to the draft report for inclusion in the final report. We presented you with the draft report dated May 22, 2015. Your written response to the draft appears in full text in the appendix of this report. We will evaluate the response and the adequacy of corrective action during a follow-up review.

We appreciate the cooperation of management and staff during our review. Please let us know if we can assist you further.

Sincerely,

Brian Ford, CIA, CISA, CRMA
Auditor-In-Charge

Debbie Banks, CFE, CICA, CMFO
Project Manager

APPROVED:

Leon Pattman, CIA, CISA, CRMA, CMFO
City Auditor

c: Distribution List

DISTRIBUTION LIST

City of Memphis

A C Wharton, Jr., Mayor

Jack Sammons, Chief Administrative Officer

Maura Sullivan-Black, Deputy Chief Administrative Officer

Jim Harvey, Deputy Chief, Police Services Division

Rowena Adams, Deputy Chief, Police Services Division

Brent Nair, Director/CIO, Information Systems Division

Memphis City Council

Edmund Ford, Jr., Audit Committee Chairman

This page left blank intentionally.

BACKGROUND

The background information provides relevant and pertinent information to assist the reader with gaining a reasonable understanding of the activity under review. Additionally, the information helps to provide the reader with the best possible context for which to understand the nature of audit findings, observations, and recommendations.

MPD uses various information technologies to effectively and efficiently carry out policing operations. Without the support of information technology, it would be very difficult for MPD to successfully carry out its mission. Therefore, since there is a substantial dependence on information technology; general controls should be designed, implemented, and monitored to provide reasonable assurance of continuous, reliable, and adequate IT support for Police operations.

Governance is a critical component of any control environment and Police's written governance is the Federal Bureau of Investigation's (FBI) Criminal Justice Information Systems (CJIS) Security Policy which as stated by management has been formally adopted beyond the CJIS networked applications. Rather, it is the policy document for the entire IT environment.

MPD has an information technology staff to manage the information technology (IT) environment that includes hardware (equipment), software (programs and applications), data (electronic records), and facilities. The information technology staff and the data center are located at the MPD's Real Time Crime Center (RTCC).

The information technology staff includes the functional roles of system administrator, database administrator, application programmer, backup administrator, and IT Support. The City Information Systems Division provides help desk support and network firewall administration.

This audit looked at IT general controls, which are those internal controls that relate to the overall IT environment, rather than to specific applications or systems. The methodology used included an evaluation of internal controls based on various IT industry standards including internal control components and principles outlined in the Control Objectives for Information and Related Technology (COBIT) framework created by ISACA (formerly the Information Systems Audit and Control Association). Additionally, we tested applicable aspects of the control environment against other audit references including the CJIS Security Policy, the City's Information Systems Security Policy, and the State of Tennessee Internal Control and Compliance Manual for Tennessee Municipalities (referred to as "City Manual" throughout this document).

OBJECTIVES, FINDINGS & RECOMMENDATIONS

OBJECTIVE 1:

To evaluate the adequacy and effectiveness of internal controls related to logical and physical security.

CONCLUSION:

Internal controls related to logical security are satisfactory but need strengthening in the areas of policies and procedures, identity management, and monitoring. Internal controls related to physical security are satisfactory.

Internal controls related to logical and physical security are those controls that provide protection from internal and external threats to the IT environment. The purpose for testing these controls is to ascertain the adequacy and effectiveness of controls to prevent and/or immediately detect security breaches. Adequate controls will help limit system downtime due to malicious attacks, unauthorized changes to hardware and software, and corruption/deletion of data that would require system shutdown and subsequent remediation and recovery. Also, some security breaches can be very expensive to fix, especially with regards to personally identifiable information.

To evaluate the adequacy and effectiveness of these controls, we conducted various tests and compared the results against various industry standards and other audit references. Generally, we tested logical security controls that included the management of user identification and passwords, monitoring of access and activity, and segregation of duties. Physical security controls we tested included controls to restrict, document and monitor access to IT facilities such as MPD's data center.

FINDINGS:

Through observation and testing, we found logical and physical security controls in place included the use of supervisory approvals of user accounts, user passwords requirement for access to network resources, and unique user identification for each user. The physical security controls included the use of locked doors, biometric entry pads, special restricted area with data center, and cameras to monitor the facilities.

Auditors evaluated the following control objectives and noted several deficiencies that should be addressed. Individually, the following are control deficiencies but if combined they could represent a significant deficiency that could allow a breach to occur and go undetected:

1) ***Monitoring:*** *- Management should periodically ensure controls are fully implemented and working effectively.*

- We did not find where MPD conducts and documents ongoing monitoring of their IT operations for indications of inappropriate, unusual, or suspicious activity. Ongoing

monitoring will allow for the detection of potential problems and improvement of controls effectiveness.

- The retention period for and review of security and incident system logs for MPD domains did not comply with the CJIS Auditing and Accountability Policy. We found that domain security logs for the domains retained activity ranging between 1 to 13 days. The CJIS Policy requires a retention period of at least one year and to continue to be retained until determined to be no longer needed; as well as weekly review of the activity on the system logs.

  NOTE: During the course of the audit, MPD purchased and implemented logging service software to address this deficiency.

2) ***Segregation of Duties:*** *- Management should limit the roles and responsibilities of individuals to reduce the likelihood that an individual could cause an error or irregularities and conceal it. Thus, the system and data could be compromised and adversely impact the organization's decision-making.*

   We identified five IT staff with potential segregation of duties conflicts based on their IT functional roles. For example, personnel performing system administrator duties also perform database administrator and backup administrator duties. If less than optimal segregation is necessary, then the affected positions should be monitored closely. As noted above, we found no deliberate monitoring activities.

3) ***Policy and Procedures:*** *- Management should develop and train employees on written procedures to implement policy to ensure individual accountability for performing assigned duties.*

   We did not find formal, written procedures for MPD IT to comply with CJIS Security Policy, Section 1.3, that requires MPD to develop, disseminate, and maintain policies and procedures to facilitate the implementation of the CJIS Security Policy and the local security policy. We did note that MPD adopted the CJIS Security Policy which serves as their governing security policy for the whole MPD IT environment.

4) ***Identity Management:*** *- Management should establish and implement controls to ensure individual accountability for all IT users.*

- Job duties and responsibilities for Police IT staff are not adequately defined in writing. For example, personnel performing in the functional roles of system administrator, backup administrator, and IT support do not have formal, written job descriptions. Therefore, it is challenging to assess if user access rights are in line with job requirements attached to user identities.

- We found 17 potential instances where user account access was not commensurate or compatible with functional job duties and responsibilities based on their stated job

duties during audit interviews. Management had not limited access rights to strictly individual job functions which could allow individuals to perform unauthorized tasks. The excess access and rights represent a control deficiency.

- All user accounts were not specifically accountable to a single individual. We found 53 generic accounts that initially did not have individual accountability and the responsibility for those accounts was not formally assigned to an individual user/person.

  NOTE: During the course of the audit, 22 of the accounts were disabled, 29 were reviewed and identified as authorized by the system administrator, and the remaining 2 were identified as benign accounts (with guest account access rights). Individual accountability for the remaining generic accounts will reside with the system administrator per management's statement.

- We found inadequate and inconsistent documentary evidence to determine that user accounts have been reviewed and approved by management in all instances. CJIS Least Privilege Policy (Section 5.5.2.1) sets minimum retention period for the documentation to one year or at least equal to agency's record retention policy. Auditors based this deficiency on the CJIS policy since it was adopted as the governing security policy.

- Terminated employee's access was not revoked in a timely manner in all instances. We found 13 active domain user accounts for employees that had been terminated during the audit period.

  NOTE: The accounts were immediately disabled by MPD IT once they were identified through the audit.

5) ***Password Management:*** *Management should design and implement controls to reduce the risk of access to systems and data by unauthorized users.*

   Default password policy was not fully implemented across the entire Police IT environment. Auditors noted that for two active domains (internal networks specifically for Organized Crime Unit and Inspectional Service Bureau) the password setting did not meet industry best practices. The complexity requirements (use of alpha, numeric, and symbols; and upper and lower case characters, etc.) were disabled and password expiration was set to 120 days rather than the industry standard of 90 days. The other domain used industry best practices for good password administration.

   NOTE: During the course of the audit, MPD adjusted default password policies on the domains to meet minimum best practices.

6) ***Physical Security:*** *Management should provide adequate safeguards for IT facilities and controlled areas to prevent and detect unauthorized access.*

- The electronic authentication directory had not been maintained adequately to ensure the authentication list was up-to-date. Auditors noted 4 data center access accounts that were not assigned to any specific, authorized individual.

  NOTE: During the course of the audit, the four identified accounts without individual accountability were removed.

- We did not find documentation that camera monitoring data are periodically reviewed to check for suspicious activity around the data center. We found that cameras electronically monitor the facilities with snapshot images which were stored on a server within the data center for approximately 30 days. However, the images were not being reviewed by anyone for suspicious activity prior to them being automatically discarded (overwritten by the cameras).

RECOMMENDATIONS:

1) ***Monitoring:***

- MPD should develop and implement a process to conduct and document ongoing monitoring and periodic management reviews of their IT operations for the purpose of evaluating the compliance to and effectiveness of controls.

- In order to meet minimum CJIS Auditing and Accountability Policy, MPD should develop and implement a process to review system logs at a minimum of once a week, retain them for at least one year and continue to retain them until determined to be no longer needed. MPD should investigate any suspicious system activity on the system logs.

2) ***Segregation of Duties:***

MPD should evaluate the duties and responsibilities of the five identified IT staff and segregate the conflicting duties, if feasible. If not, MPD should mitigate the risk by effectively and routinely monitoring the activities of the staff that have improperly segregated duties and system access.

3) ***Policy and Procedures:***

- MPD should develop, disseminate, and maintain procedures to facilitate the implementation of the CJIS Security Policy requirements.

- The procedures should provide specific guidance on how to document compliance with the CJIS Security Policy.

*4) **Identity Management:***

- MPD should formally develop written documentation of duties and responsibilities for employees serving in IT functional roles.

- MPD should review each of the 17 identified potential user access account exceptions and make sure the access granted is limited to their daily duties. In certain circumstances, additional access should be granted on an as-needed basis and removed when no longer needed. Additionally, management should make sure the appropriate level of monitoring occurs where there is elevated risk due to elevated privileges.

- MPD should put a process in place to manage service accounts and other non-person accounts to provide for individual accountability for all activities performed by the accounts. Accounts that are not required and used on a daily basis should be inactive and when activated, the security administrator should be monitoring the account usage.

- MPD should develop and implement policies and procedures for user account approval that includes documentation requirements and the retention of the documentation while the user has access.

*5) **Password Management:***

No recommendation warranted—management corrected the deficiency regarding the default password policy during the course of the audit.

*6) **Physical Security:***

Develop and implement a process to periodically review camera monitoring data to check for suspicious activity around the data center. We recommend this be done in conjunction with periodic (weekly) review of audit logs or at least within the period prior to camera snapshots being overwritten.

OBJECTIVE 2:

To evaluate the adequacy and effectiveness of internal controls related to application / system development and maintenance.

CONCLUSION:

Internal controls related to application system development and maintenance are satisfactory with opportunities for improvement.

Internal controls related to application/system development and maintenance are those controls that help ensure that appropriate applications/systems are designed, developed, tested, implemented, and maintained through their entire life cycle. The overarching objectives are to ensure adequate technology support for operations via ongoing system availability, stability, and reliability.

To evaluate the adequacy and effectiveness of these controls, we conducted various tests and compared the results against various industry standards and other audit references. Generally, we evaluated MPD's applications system development and maintenance environment by reviewing documentation supporting their software development life cycle (SDLC) and maintenance scheduling.

FINDINGS:

We observed that the MPD IT operation includes a function for their application development and maintenance. Generally they follow a project methodology consistent with COBIT best practices, the CJIS Security Policy, and the City's IS Security Policy. Examples include conducting system requirements analysis using the City's procurement process, including user personnel in new system development (acquisition), and considering audit and security concerns during the initial analysis phase. We observed, however, the following opportunities for improvement:

- MPD has not developed and implemented written policies and procedures for the application development environment. Written policies and procedures will assist MPD in developing, managing, and maintaining applications through all phases of the SDLC in a controlled way. Generically, these phases are requirements, design, build/code, test, implementation, and maintenance.

- We did not find that MPD routinely and consistently maintains adequate documentation of systems, applications, operating system, and configurations throughout the SDLC. Additionally, we did not find sufficient, written documentation such as plans/schedules for routine maintenance to ensure maintenance is conducted in a timely manner.

RECOMMENDATION:

MPD should develop and implement formal application system development and maintenance policies and procedures that at a minimum meet the requirements of the CJIS Security Policy and the City's IS Security Policy, as well as industry SDLC methodologies. Their chosen methodology should require documentation of SDLC phases (including maintenance plans and schedules) and adequate records retention.

OBJECTIVE 3:

To evaluate the adequacy and effectiveness of internal controls related to change management.

CONCLUSION:

Internal controls related to change management are satisfactory with opportunities for improvement.

Change management controls help ensure the availability, stability and reliability of technology support systems by preventing unauthorized and untested changes to the IT environment. The change management process provides controls for planned and emergency changes to IT system hardware configurations, software applications, and operating systems. Planned changes include software updates, routine system maintenance, and minor upgrades. Emergency changes include break-fixes due to a variety of reasons. Adequate controls will help protect the "live" production environment from unneeded changes, programming errors, unnecessary system downtime, and complete system failure that could compromise overall data reliability needed for decision-making.

To evaluate the adequacy and effectiveness of these controls, we conducted various tests and compared the results against various industry standards and other audit references. Generally, we evaluated MPD's change management process for planned non-emergency and emergency changes to their applications and systems.

FINDINGS:

We observed that MPD follows an informal change management process to control changes to their information systems. Their process includes good practices such as testing system changes prior to moving the changes to the production environment and using a small group of users to evaluate/test system changes. The following areas need improvement, however, to limit the risks associated with these changes:

- We did not find that MPD has developed and implemented written change management policies and procedures per COBIT best practices and as required by the CJIS Security Policy.

- We did not find adequate documentation that MPD systematically catalogs and tracks changes to the IT environment, i.e. hardware configurations, applications, operating systems, etc.

RECOMMENDATIONS:

MPD should develop and implement written policies and procedures to document their change management process. The procedures should meet the minimum requirements of the CJIS Security Policy and include but not be limited to:

- Procedures to obtain appropriate management approval for all changes (including emergencies).
- Procedures to handle in a standardized manner all requests (including maintenance and patches) for changes to applications, procedures, processes, and system parameters.
- Procedures for defining, testing, documenting, assessing and authorizing emergency changes that do not follow the established change process. Ensure that approved changes are implemented as planned.
- Procedures to verify whenever changes are implemented, that the associated system and user documentation and end-user procedures are updated accordingly.
- Procedures to reverse changes in case of failure.
- Procedures to catalog all changes to their IT environment, including hardware configurations, applications, and operating systems. Records should be retained and maintained in accordance with the CJIS Security Policy.

OBJECTIVE 4:

To evaluate the adequacy and effectiveness of internal controls related to disaster recovery.

CONCLUSION:

Internal controls related to disaster recovery are inadequate to provide for timely and organized resumption of IT operations and is a material weakness regarding the IT control environment.

Disaster recovery controls enable the organization to recover in the event of a local or regional disaster or from a major disruption of operations in a planned and organized, timely manner. The plan is intended to help ensure the availability and adequate safeguarding of critical backup IT hardware, software, operating systems, data, guidance, and human resources.

To evaluate the adequacy and effectiveness of these controls, we conducted various tests and compared the results against various industry standards and other audit references. Generally, we tested for the adequacy of MPD's disaster recovery planning as it relates to their data center, which included reviewing the City's overall disaster recovery plan as it relates to MPD, to determine if the plans would enable MPD to resume critical IT operations in a timely manner. Finally, we assessed MPDs current data backup process as it relates to disaster recovery.

FINDINGS:

Through observation and interviews, we found that MPD has completed some IT disaster recovery planning and is coordinating with City IS to be included in the City-wide plan, although planning is not complete. Some data, such as MPD email, are backed up as part of the City's backup process, but all critical MPD data is not currently backed up to an offsite facility; preferably outside the radius of any defined regional disaster.

Auditors noted the following deficiencies:

- MPD does not have an approved, tested, and disseminated Disaster Recovery/Business Continuity plan in place as required by the City Manual to reduce the impact of a disaster or major disruption on key Police functions and processes, i.e. MPD is not protected from a regional disaster or major disruption. Examples of basic items in a plan include:
    - Inventory of critical data, applications, and hardware
    - Contact list of key personnel
    - Off-site backups/replication of critical data

- Regular restore testing of critical data
- Regular updates to the plan

- MPD is not currently backing up critical data offsite as required by the City Manual. Critical data collected and stored by MPD at the RTCC data center is currently backed up to a storage area network (SAN) device within the RTCC data center, i.e. MPD is not protected from a local disaster or major disruption.

RECOMMENDATIONS:

- MPD should continue to work with City IS to complete the development and implementation of a MPD IT Disaster Recovery/Business Continuity plan that includes the replication of MPD critical data to the City's disaster recovery site. Until a formal plan is in place, MPD should work with City IS to develop and issue interim guidance as soon as feasible.

- MPD should immediately backup all systems and data to an offsite location.

OBJECTIVE 5:

To evaluate the adequacy and effectiveness of internal controls related to environmental controls.

CONCLUSION:

Internal controls are satisfactory to minimize the potential impact on environmental risks.

Internal controls related to environmental controls are those controls that protect critical IT assets from environmental hazards such as fires, floods, excessive temperature and humidity, loss of power, etc. Adequate controls will help ensure critical IT assets exposed to environmental impacts remain available, prevent and/or minimize damage, comply with health and safety regulations, prevent outages due to power interruptions, and prevent accidents to personnel.

To evaluate the adequacy and effectiveness of these controls, we conducted various tests and compared the results against various industry standards and other audit references. Generally, we evaluated the data center environment, which contains critical MPD IT assets, to determine if it included adequate environmental control systems such as fire detection and suppression systems; smoke, heat, and flame detectors; cooling systems and humidifiers; backup generator, uninterruptible power supply (UPS) battery backup system, etc. We also inspected the data center to determine if it was free from environmental hazards such as debris, flammable liquids, etc. and if it was at risk of flooding.

FINDINGS:

Through observation and inspection of the data center environment, we found the devices and equipment in use to be adequate to protect the computer equipment and personnel from environmental factors. We found:

- Data center is not at a significant risk of flooding.
- Smoke and fire alarm with fire suppression system is in place to protect the data center.
- Diesel-powered backup generator provides auto-activated power when needed. The generator is tested weekly.
- UPS battery bank provides temporary power for controlled system shut-down and switch-over to generator.
- Data center is cooled by two cooling units.

Opportunities for Improvement:

- UPS batteries have been in use for approximately six years. Consider replacing since they are beyond the expected 5-year life.

- Consider updating to the explosion proof model of the electric control device that releases the fire suppressant agent in a fire emergency. The current model is CPYEC-24 and the explosion proof model is CPYEC-24-EXP which would reduce the risk of injury to employees due to metal debris from the potential explosion if activated.

RECOMMENDATION:

Management should consider taking advantage of the opportunities for improvement.

APPENDIX

Response from Director of Police Services

City of Memphis
TENNESSEE

A C WHARTON, JR. - Mayor
JACK SAMMONS - Chief Administrative Officer
DIVISION OF POLICE SERVICES
TONEY C. ARMSTRONG - Director

August 7, 2015

Leon Pattman, City Auditor
City of Memphis
125 N. Main Street, Suite 536
Memphis, Tennessee 38103

Dear Mr. Pattman,

Please find attached the Memphis Police Department's (MPD) Corrective Action Plan for the "Police IT General Controls Audit Report". The Memphis Police Department has reviewed the audit and is working to make corrective action as shown in the attached document. MPD's IT Department will work closely with the City of Memphis IT Department to resolve all issues in a timely manner. Weekly review of all action items will be held by Deputy Chief Jim Harvey until all items have been corrected.

Thank you,

Toney C. Armstrong
Director of Police Services
City of Memphis

Police IT General Controls Audit
CORRECTIVE ACTION PLAN MANAGEMENT TRACKING TOOL
Prepared by:
As of: June 30, 2015

	CONTROL DEFICIENCY	AUDIT RECOMMENDATION	RESPONSIBLE PARTY	PLANNED CORRECTIVE ACTION	DUE DATE	CURRENT STATUS	DATE COMPLETED
1	We did not find where MPD conducts and documents ongoing monitoring of their IT operations for indications of inappropriate, unusual, or suspicious activity.	MPD should develop and implement a process to conduct and document ongoing monitoring and periodic management reviews of their IT operations for the purpose of evaluating the compliance to and effectiveness of controls.	MPD Information Services	MPD IT will establish policies, procedures, and processes for identifying, monitoring unusual or potentially suspicious activity, and documenting it as appropriate.	8/28/2015	In Process	
2	The retention period for and review of security and incident system logs for MPD domains did not comply with the CJIS Auditing and Accountability Policy.	In order to meet minimum CJIS Auditing and Accountability Policy, MPD should develop and implement a process to review system logs at a minimum of once a week, retain them for at least one year and continue to retain them until determined to be no longer needed. MPD should investigate any suspicious system activity on the system logs.	MPD Information Services	MPD IT will develop policies that clearly define mandatory requirements and suggested recommendations for log management activities, including log generation, transmission, storage, analysis, and disposal. MPD IT will ensure that related policies and procedures incorporate and support the log management requirements and recommendations. management will provide the necessary support for the efforts involving log management planning, policy, and procedures development.	12/17/2015	In Process	
3	We identified five IT staff with potential segregation of duties conflicts based on their IT functional roles.	MPD should evaluate the duties and responsibilities of the five identified IT staff and segregate the conflicting duties, if feasible. If not, MPD should mitigate the risk by effectively and routinely monitoring the activities of the staff that have improperly segregated duties and system access.	MPD Information Services	MPD IT will establish policies, procedures, and processes to segregate duties wherever possible and assign an appropriate mitigation control in cases wherein it is feasible to do so. In addition, these controls will be monitored on a quarterly basis and the results reported to senior management.	11/10/2015	In Process	
4	We did not find formal, written procedures for MPD IT to comply with CJIS Security Policy, Section 1.3, that requires MPD to develop, disseminate, and maintain policies and procedures to facilitate the implementation of the CJIS Security Policy and the local security policy.	MPD should develop, disseminate, and maintain procedures to facilitate the implementation of the CJIS Security Policy requirements. The procedures should provide specific guidance on how to document compliance with the CJIS Security Policy.		MPD IT will develop, disseminate, and maintain formal, documented procedures to facilitate the implementation of the CJIS Security Policy and, where applicable, the local security policy. The policies and procedures shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance.	12/31/2015	In Process	

Date
4:07 PM

Police IT General Controls Audit
CORRECTIVE ACTION PLAN MANAGEMENT TRACKING TOOL
Prepared by:
As of: June 30, 2015

	CONTROL DEFICIENCY	AUDIT RECOMMENDATION	RESPONSIBLE PARTY	PLANNED CORRECTIVE ACTION	DUE DATE	CURRENT STATUS	DATE COMPLETED
5	Job duties and responsibilities for Police IT staff are not adequately defined in writing.	MPD should formally develop written documentation of duties and responsibilities for employees serving in IT functional roles.		MPD IT senior management will develop job(s) specifications details the skills, experience, abilities and expertise that are required to do the job(s) and the roles and responcibilities for the job(s).	11/10/2015	In Process	
6	We found 17 potential instances where user account access was not commensurate or compatible with functional job duties and responsibilities based on their stated job duties during audit interviews.	MPD should review each of the 17 identified potential user access account exceptions and make sure the access granted is limited to their daily duties.		MPD IT will develp written documentation of duties and responsibilities for employees, appropriate account access will be granted and limited according to daily duties.	11/10/2015	In Process	
7	All user accounts were not specifically accountable to a single individual.	MPD should put a process in place to manage service accounts and other non-person accounts to provide for individual accountability for all activities performed by the accounts.		MPD IT management will monitor account creation and monitor account access to the system(s).	9/18/2015	In Process	
8	We found inadequate and inconsistent documentary evidence to determine that user accounts have been reviewed and approved by management in all instances.	MPD should develop and implement policies and procedures for user account approval that includes documentation requirements and the retention of the documentation while the user has access.	MPD Information Services	Memphis Police Department Information Systems is currently in the process of developing and implementing policies and procedures for user account approval that includes documentation requirements and the retention of the documentation while the user has access. Once developement and drafting is complete these procedures will be submitted in written from for approval.	9/18/2015	In Process	
9	Terminated employee's access was not revoked in a timely manner in all instances.		MPD Information Services	MPD IT will establish policies, procedures, and processes for disabling terminated employees accounts.	8/7/2015	Complete	8/7/2015
10	Default password policy was not fully implemented across the entire Police IT environment.	No recommendation warranted—management corrected the deficiency regarding the default password policy during the course of the audit.				Complied during original Audit	
11	The electronic authentication directory had not been maintained adequately to ensure the authentication list was up-to-date.		MPD Information Services	MPD IT will establish policies, procedures, and processes for identifying, monitoring the electronic authentication and directory.	8/18/2015	In Process	
12	We did not find documentation that camera monitoring data are periodically reviewed to check for suspicious activity around the data center.	Develop and implement a process to periodically review camera monitoring data to check for suspicious activity around the data center.	MPD Information Services	MPD IT will establish policies, procedures, and processes for identifying, monitoring and reviewing camera feeds for activity.	8/31/2015	In Process	

Police IT General Controls Audit
CORRECTIVE ACTION PLAN MANAGEMENT TRACKING TOOL
Prepared by:
As of: June 30, 2015

	CONTROL DEFICIENCY	AUDIT RECOMMENDATION	RESPONSIBLE PARTY	PLANNED CORRECTIVE ACTION	DUE DATE	CURRENT STATUS	DATE COMPLETED
13	MPD has not developed and implemented written policies and procedures for the application development environment.	MPD should develop and implement formal application system development and maintenance policies and procedures that at a minimum meet the requirements of the CJIS Security Policy and the City's IS Security Policy, as well as industry SDLC methodologies. Their chosen methodology should require documentation of SDLC phases (including maintenance plans and schedules) and adequate records retention.	MPD Information Services	MPD IT will establish formal application system development and maintenance policies and procedures , to facilitate the implementation of the CJIS Security Policy and, where applicable, the local security policy. that at a minimum meet the requirements City's IS Security Policy, as well as industry SDLC	9/10/2015	In Process	
14	We did not find that MPD routinely and consistently maintains adequate documentation of systems, applications, operating system, and configurations throughout the SDLC.		MPD Information Services	MPD IT will establish formal application system development and maintenance policies and procedures , to facilitate the implementation of the CJIS Security Policy and, where applicable, the local security policy. that at a minimum meet the requirements City's IS Security Policy, as well as industry SDLC	12/4/2015	In Process	
15	We did not find that MPD has developed and implemented written change management policies and procedures per COBIT best practices and as required by the CJIS Security Policy.	MPD should develop and implement written policies and procedures to document their change management process. The procedures should meet the minimum requirements of the CJIS Security Policy and include but not be limited to:	MPD Information Services	Memphis Police Department Information Systems is currently in the process of developing and implementing policies and procedures to document their change management process. The procedures should meet the minimum requirements of the CJIS Security Policy and include but not be limited to:	9/25/2015	In Process	
		Procedures to obtain appropriate management approval for all changes (including emergencies).	MPD Information Services	Memphis Police Department Information Systems is currently in the process of developing & drafting procedures to obtain appropriate management approval for all changes (including emergencies). Once developement and drafting is complete these procedures will be submitted in written form for approval.	9/25/2015	In Process	
		Procedures to handle in a standardized manner all requests (including maintenance and patches) for changes to applications, procedures, processes, and system parameters.	MPD Information Services	Memphis Police Department Information Systems is currently in the process of developing & drafting procedures to handle in a standardized manner all requests (including maintenance and patches) for changes to applications, procedures, processes, and system parameters. Once developement and drafting is complete these procedures will be submitted in	9/25/2015	In Process	

Police IT General Controls Audit
CORRECTIVE ACTION PLAN MANAGEMENT TRACKING TOOL
Prepared by:
As of: June 30, 2015

	CONTROL DEFICIENCY	AUDIT RECOMMENDATION	RESPONSIBLE PARTY	PLANNED CORRECTIVE ACTION	DUE DATE	CURRENT STATUS	DATE COMPLETED
		Procedures for defining, testing, documenting, assessing and authorizing emergency changes that do not follow the established change process. Ensure that approved changes are implemented as planned.	MPD Information Services	Memphis Police Department Information Systems is currently in the process of developing & drafting procedures for defining, testing, documenting, assessing and authorizing emergency changes that do not follow the established change process. Ensure that approved changes are implemented as planned. Once developed and drafting is complete these procedures will be submitted in written for approval.	9/25/2015	In Process	
		Procedures to verify whenever changes are implemented, that the associated system and user documentation and end-user procedures are updated accordingly.	MPD Information Services	Memphis Police Department Information Systems is currently in the process of developing & drafting procedures to verify whenever changes are implemented, that the associated system and user documentation and end-user procedures are updated accordingly. Once developed and drafting is complete these procedures will be submitted in written form for approval.	9/25/2015	In Process	
		Procedures to reverse changes in case of failure.					
16	We did not find adequate documentation that MPD systematically catalogs and tracks changes to the IT environment, i.e. hardware configurations, applications, operating systems, etc.	Procedures to catalog all changes to their IT environment, including hardware configurations, applications, and operating systems. Records should be retained and maintained in accordance with the CJIS Security Policy.	MPD Information Services	Memphis Police Department Information Systems is currently in the process of developing & drafting procedures to catalog all changes to their IT environment, including hardware configurations, applications, and operating systems. Records should be retained and maintained in accordance with the CJIS Security Policy. Once developed and drafting is complete these procedures will be submitted in written for approval.	11/20/2015	In Process	
17	MPD does not have an approved, tested, and disseminated Disaster Recovery/Business Continuity plan in place as required by the City Manual to reduce the impact of a disaster or major disruption on key Police functions and processes, i.e. MPD is not protected from a regional disaster or major disruption.	MPD should continue to work with City IS to complete the development and implementation of a MPD IT Disaster Recovery/Business Continuity plan that includes the replication of MPD critical data to the City's disaster recovery site. Until a formal plan is in place, MPD should work with City IS to develop and issue interim guidance as soon as feasible.	MPD Information Services	MPD shall continue to work with City IS to complete the development and implementation of a MPD IT Disaster Recovery/Business Continuity plan that includes the replication of MPD critical data to the City's disaster recovery site. Until a formal plan is in place, MPD should work with City IS to develop and issue interim guidance as soon as feasible.	10/31/2015	In Process	

Police IT General Controls Audit
CORRECTIVE ACTION PLAN MANAGEMENT TRACKING TOOL
Prepared by:
As of: June 30, 2015

	CONTROL DEFICIENCY	AUDIT RECOMMENDATION	RESPONSIBLE PARTY	PLANNED CORRECTIVE ACTION	DUE DATE	CURRENT STATUS	DATE COMPLETED
18	MPD is not currently backing up critical data offsite as required by the City Manual.	MPD should immediately backup all systems and data to an offsite location.	MPD Information Services	MPD IT is in the process of setting up the offsite backup environment to off site location this should be complete approximately 9/15/2015.	10/31/2015	In Process	