CITY AUDITOR'S OFFICE

Police Technology Services

August 4, 2020 AUDIT REPORT NO. 2003

August 4, 2020

Honorable Mayor and Members of the City Council:

Enclosed is the audit report for *Police Technology Services*, which was included on the Council-approved FY 2019/20 Audit Plan as a contracted information technology audit. We contracted with MGT of America Consulting, LLC, to perform an evaluation of the effectiveness of internal controls over Police information technology.

The audit found that more formalized roles and responsibilities between the Police Technology Services Division and the City's Information Technology department would help strengthen technology controls. As well, the existing continuity of operations plan could be updated and expanded, including incident response policies and procedures. Additionally, controls related to access and change management could be improved.

If you need additional information or have any questions, please contact me at (480) 312-7867.

Sincerely,

Sharron Walker

Sharron E. Walker, CPA, CFE, CLEA
City Auditor

Audit Team:

Paul Christiansen, CPA, CIA – Sr. Auditor
Lai Cluff, CIA – Sr. Auditor

TABLE OF CONTENTS

AUDIT HIGHLIGHTS

Police Technology Services

August 4, 2020 Audit Report No. 2003

WHY WE DID THIS AUDIT

An audit of *Police Technology Services* was included on the City Council-approved fiscal year (FY) 2019/20 Audit Plan as a contracted information technology (IT) audit. We contracted with MGT of America Consulting, LLC, to evaluate the effectiveness of internal controls over Police information technology.

BACKGROUND

The Technology Services Division (TSD) within the Police Department's Operational Support Bureau provides support for the specific systems and equipment used by the department's approximately 660 full-time equivalent (FTE) employees. TSD works in cooperation with the City's IT department, which manages technology infrastructure, including the citywide network, systems and information security.

This audit reviewed the Police Department's IT general controls, which are basic controls that apply to all systems, such as access controls, change management, and backup and recovery processes.

As a law enforcement agency, the department must comply with the FBI's Criminal Justice Information Services Security Policy, which provides minimum security requirements for the handling of criminal justice information.

City Auditor's Office

City Auditor 480 312-7867
Integrity Line 480 312-8348
www.ScottsdaleAZ.gov

WHAT WE FOUND

More formalized roles and responsibilities between TSD and City IT would help strengthen controls.

A service-level agreement between the department and City IT would help ensure requirements are addressed and security controls established. As well, expanded continuity of operations and incident response planning is needed, including periodic testing of backup and recovery processes to ensure integrity and availability of data.

Controls related to access and change management could be improved.

To protect the confidentiality, integrity, and availability of Police Department data, access to equipment and software applications should be limited on a least-privilege basis. We found:

- For 6 out of 10 Police employees separated within the past year, notification to City IT or Municipal Security occurred 1 to 7 days after the separation dates.
- Centralized user access information could make the process of notifying department system administrators of employee separations more efficient.
- Access to server rooms should be reviewed and further restricted.

As well, policies and procedures for testing and documenting program changes are not formalized.

WHAT WE RECOMMEND

The Technology Services Division:

- Work with City IT to establish a service-level agreement and update and expand on the existing continuity of operations plan.
- Establish procedures to timely deactivate separated employees' access, review and further restrict server room access, and establish policies and procedures for testing and documenting program changes.

MANAGEMENT RESPONSE

The department agreed with the recommendations and plans to complete implementation by February 2021.

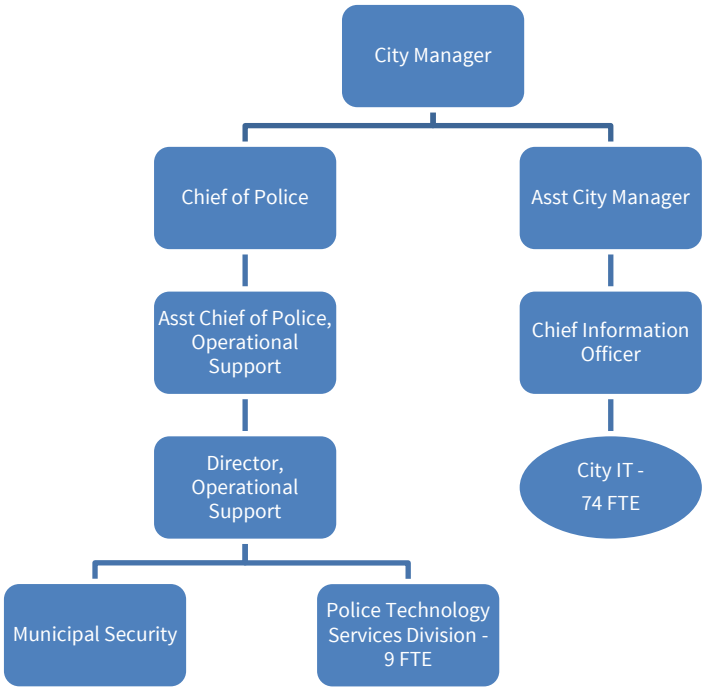
BACKGROUND

This audit of Police Technology Services was included on the City Council-approved fiscal year (FY) 2019/20 Audit Plan as a contracted information technology (IT) audit. The audit objective was to evaluate the effectiveness of internal controls over Police information technology. We contracted with MGT Consulting to perform an evaluation of the department's IT general controls.

IT General Controls are basic controls that apply to all systems, such as access controls, change management, and backup and recovery processes.

The Technology Services Division (TSD) within the Police Department's Operational Support Bureau provides support for the specific systems and equipment used by the department's approximately 660 full-time equivalent (FTE) employees. The department staffs two system integration supervisors and seven system integrators, under the direction of a Director. The Police Technology Services Division works in cooperation with the City's IT department, which manages the City's technology infrastructure, including the citywide network, systems and information security. TSD, like other departmental technology groups, follows the general technology policies established by the City's IT department.

Figure 1. Police Technology Services, Organizational Structure



SOURCE: Auditor analysis of the City organizational chart, department organizational structure, and the FY 2019/20 Adopted FTE Budget.

Police Technology

The Police Department uses more than 100 different software applications across its various operational units. The Technology Services Division provides user support for many of these applications and helps maintain the servers, hardware, and equipment used with these applications.

Audit specialists evaluated the department's IT general controls using the following standards:

- CJIS Security Policy — As a law enforcement agency, the Scottsdale Police Department creates, receives, stores, and transmits criminal justice information (CJI) and must follow the minimum requirements set forth by the Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) Security Policy. The essential premise of the CJIS Security Policy is to provide appropriate controls to project CJI data, whether at rest or in transit. All entities handling CJI must comply with these minimum standards, but local policy may expand on the standards.
- ISO 27001 — standards for an information security management system established by the International Organization for Standardization (ISO). Using the standards can help an organization to manage the security of assets such as financial assets, employee details, or information entrusted by a third party.
- COBIT®5 (Control Objectives for Information and Related Technology) — developed by ISACA as a comprehensive framework for the governance and management of information technology. The framework is based on principles such as meeting stakeholder needs and applying a single integrated framework aligned with other IT-related standards.

The **CJIS Security Policy** provides minimum security requirements associated with the creation, viewing, modification, transmission, dissemination, storage, or destruction of criminal justice information. Examples include:

- Biometric data
- Biographic data
- Property Data
- Case/Incident History
- Criminal History

SOURCE: FBI CJIS Security Policy, ver. 5.8

OBJECTIVES, SCOPE, AND METHODOLOGY

This audit of *Police Technology Services* was included on the City Council-approved fiscal year (FY) 2019/20 Audit Plan as a contracted information technology (IT) audit. The audit objective was to evaluate the effectiveness of internal controls over Police information technology.

We contracted with MGT of America Consulting, LLC (MGT) as IT audit specialists to conduct the audit of general IT controls impacting the Police Department systems. As required by Government Auditing Standards, we evaluated the qualifications and independence of the specialists and documented the objectives and scope of their work, the intended use of their work to support the audit objectives, and their procedures and findings.

To gain an understanding of the general IT controls impacting the Police Department systems, MGT reviewed:

- Criminal Justice Information Services (CJIS) Security Policy established by the Criminal Justice Information Services Division of the Federal Bureau of Investigation
- Policies, procedures, roles and responsibilities of the Police Department's Technology Services Division (TSD) and City IT related to Police information technology internal controls

Auditors interviewed the Police Department operational support director and supervisors responsible for Police Technology Services, as well as City IT's chief information security officer, IT director over infrastructure, and IT director over applications.

To meet the audit objectives, auditors performed the following procedures:

- Evaluated controls over the physical security of the computer equipment
- Assessed controls over access to the various Police Department systems
- Reviewed procedures for controlling program changes through IT management and programming personnel
- Reviewed procedures related to backup and recovery controls
- Tested systems development and acquisition controls
- Assessed computer operations controls
- Evaluated controls to protect data against unauthorized access or manipulation
- Reviewed telecommunication controls
- Assessed network controls
- Reviewed controls and procedures related to personal computers
- Assessed internet and electronic commerce controls

The audit specialists used best practices and standards from COBIT® 5 standards for governance and management of enterprise IT, the National Institute of Standards and Technology (NIST), the CJIS Security Policy, and the International Organization for Standardization's standard for Information Technology (ISO 27001, Information Security Management) to evaluate general IT controls impacting the Police Department systems.

Overall, auditors concluded that more formalized roles and responsibilities between the department's TSD and City IT would help strengthen technology controls, and controls over access and change management could be improved.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Audit work took place from January to June 2020.

FINDINGS AND ANALYSIS

1. More formalized roles and responsibilities between TSD and City IT would help strengthen controls.

The CJIS Security Policy places responsibility on the Police Department for managing the security of the criminal justice information it creates, stores, and transmits. As such, a service level agreement between the department's Technical Services Division (TSD) and the City's Information Technology (City IT) department would help ensure that requirements are being addressed and security controls established.

A. Roles and responsibilities between the TSD and City IT should be formalized to ensure adequate coverage of technology risks.

The Police Technology Services Division works cooperatively with and relies on the City's IT department to manage and support the technology infrastructure. However, given the sensitive and critical nature of certain Police systems and TSD's responsibility in managing the risks related to their specific systems, the department needs to be fully aware of how risks are being mitigated and each party's role in that process.

City IT is responsible for infrastructure services such as, database management, firewall access, network monitoring, and telecommunications. But, to fully comply with CJIS standards, TSD needs to be aware of and verify that the described controls are functioning. As well, the groups should agree on the level of communication expected for issues and monitoring results.

B. Expanded continuity of operations and incident response planning is needed.

Certain components of incident response and disaster recovery are performed by City IT, and TSD will need to work with City IT to identify and coordinate each group's responsibilities.

1. Continuity of operations plan (COOP) needs to be updated annually and expanded to include risk analysis, arrangements with vendors to support the needed hardware and software requirements, and forms or documents needed.

The department's COOP was last updated September 2017 and some key contacts have since changed or left City employment. While the plan identifies alternate facilities for use in case of disaster, it does not identify critical applications, hardware, and equipment. A more thorough risk analysis is needed to identify the critical applications, the potential exposures, and impact to the City if these applications are inaccessible during a disaster. As well, the plan does not identify forms or other control documents that will be needed during a disaster when IT systems may not be available. The department's risk assessment and disaster recovery planning should also take into consideration systems that are not part of City IT's backup and recovery process, such as the crime lab systems.

Within the last few years, the City's IT department has established an offsite data center and has been working on disaster recovery planning. TSD relies on the City IT to manage this process; however, CJIS standards places the responsibility of managing the approved security requirements on the agency administering criminal justice. Therefore, being aware of the recovery process and TSD's role in that process helps fulfill the responsibility.

As well, CJIS guidance states that agencies should obtain an understanding of its vendors' and service providers' contract provisions relating to continuity planning and disaster recovery, to ensure that critical operations can be immediately resumed, and operations can be eventually reinstituted in a timely and organized manner.

Additionally, once established, the department should be involved in testing the COOP and disaster recovery plans.

Periodically, the department should test backup and recovery controls needed to ensure integrity and availability of data. The City's IT department performs data backup and recovery functions for City departments, including Police. Data is stored on data domains in two different locations, and City IT periodically takes inventory to verify that the appropriate backup files are being maintained. However, given the potential criticality of certain Police data, periodically testing the integrity of the data backups can provide assurance they will work when needed.

2. Incident response policies and procedures are needed.

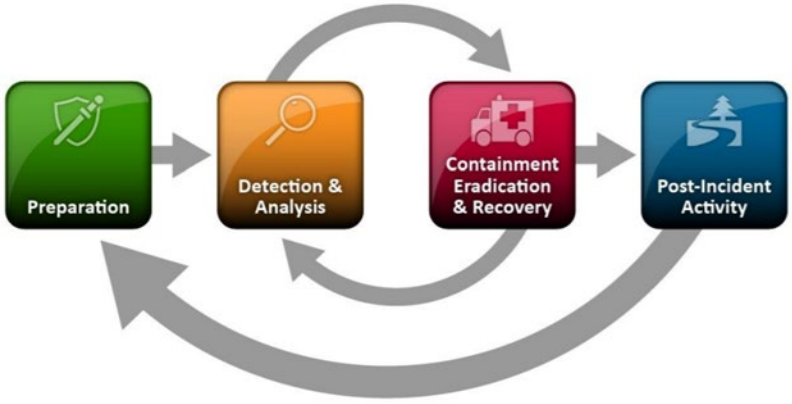
   TSD primarily relies on City IT to communicate security incidents and manage the incident response. TSD has not yet developed a department-level incident response plan to provide its staff consistent direction for handling security incidents.

   Examples of security incidents include ransomware execution, denial of service attacks, data exfiltration, and unauthorized access to systems. While City IT's monitoring services will detect many incidents first, other users throughout the Police Department network may detect security incidents. TSD staff needs to understand signs of security issues and be prepared with the critical actions to take and where to report the potential incidents.

   CJIS Security Policy requires that agencies establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities. As well, incidents must be documented and reported to the appropriate authorities. These standards are based on guidance from the National Institute of Standards and Technology (NIST). Figure 2, on page 9, summarizes incident response activities as illustrated in the NIST *Incident Response Life Cycle* diagram.

(continued on next page)

Figure 2. NIST Incident Response Life Cycle



SOURCE: NIST Special Publication 800-61, rev.2, *Computer Security Incident Handling Guide.*

Recommendations:

The Police Chief should require TSD to:

A. Work with City IT to establish a service level agreement that details the roles and responsibilities of each department in managing technology risks.

B. Update and expand on the existing Continuity of Operations Plan, including performing risk assessment, identifying critical technology systems, testing backup and recovery processes, and establishing incident response policies and procedures.

2. Controls related to access and change management could be improved.

To protect the confidentiality, integrity, and availability of Police Department data, access to equipment and software applications should be limited on a least-privilege basis. That is, access should only be provided to those needing it to carry out their job responsibilities. Testing and documentation of program changes could also be improved.

A. Access to the City's network, Police systems and facilities need to be more promptly deactivated after employee termination. Also, TSD does not centrally maintain information regarding each user's system access, including authorizations, changes, and deactivation of user accounts.

1. For 6 out of 10 randomly selected Police employees separated within the past year, notification to City IT or Municipal Security occurred 1 to 7 days after the separation dates. In three other instances, facility badge access was deleted up to 2 months after the employee separation, and the department could not confirm whether access was disabled at an earlier date.

2. TSD did not have written procedures requiring that system administrators be notified of employee separations so that system access could be removed. Accordingly, for the two tested systems, access deactivation was not timely.

   - For one system, account deactivation for 3 of the 10 selected employees occurred 4 to 6 days after the separation dates.
   - In the second system, 13 of the 55 employees who separated within the last year still had active accounts.

   Further, the department has several cloud-based applications. Unlike applications hosted on the City's network, cloud-based applications may be accessed from any computer through an internet connection. Deactivating network access does not end the former employee's access to cloud-based applications; therefore, it is even more critical that the application-specific access is removed.

Requiring prompt notification of employee separations by the applicable Police Department staff to City IT, TSD and Municipal Security staff can help minimize the risk of unauthorized system access. And centralized user access information will make the process more efficient.

B. Access to server rooms should be reviewed and further restricted.

Besides TSD personnel, the department's computer server rooms were accessible to Police management and certain other personnel, including Police Communications staff, Fire Department management, IT staff, facilities maintenance technicians, and several visitor badges. However, to limit the risk of unauthorized changes, damage to equipment, or theft of data, computer room access should be restricted on a least-privilege basis with other persons being escorted when access is required.[1] Additionally, if the Police Department authorizes direct access for non-Police staff, CJIS-required background checks have to be completed. As well, more security cameras and locked server cabinets would provide further protection for the department's technology.

C. Change control policies, including documentation of changes and testing are needed.

TSD did not have policies and procedures requiring program changes to be tested and test methodology and results to be reviewed and approved before technology changes are implemented. For 3 systems selected for review, TSD did not provide documentation to show that program changes had been tested before implementation. Specific program change controls are needed to identify, document, and authorize changes to IT systems before the systems are modified and changes put into operation.

Recommendations:

The Police Chief should require TSD to:

A. Work with other Police Department units to establish policies and procedures to ensure timely deactivation of separated employees' access and centralize user access information, including authorizations to add, change, or remove user access.

[1] Least-privilege basis means that only those individuals needing access to perform their regular job duties should be granted access, and it should only be the necessary access level to perform those duties.

B. Review existing access to department server rooms and restrict access on a least-privilege basis.

C. Establish policies and procedures for change management, including authorization, documentation and verification of program changes.

MANAGEMENT ACTION PLAN

1. More formalized roles and responsibilities between TSD and City IT would help strengthen controls.

Recommendations:

The Police Chief should require TSD to:

A. Work with City IT to establish a service level agreement that details the roles and responsibilities of each department in managing technology risks.

B. Update and expand on the existing Continuity of Operations Plan, including performing risk assessment, identifying critical technology systems, testing backup and recovery processes, and establishing incident response policies and procedures.

MANAGEMENT RESPONSE: Agree

PROPOSED RESOLUTION:

A. TSD will work directly with City IT via a series of meetings in establishing a service level agreement that details the roles and responsibilities of each department in managing technology risks.

B. TSD will update the existing Continuity of Operations Plan to include performing risk assessment, identifying critical technology systems, testing backup and recovery processes, and establishing incident response policies and procedures in partnership with City IT.

RESPONSIBLE PARTY: Director Michael Keran

COMPLETED BY: 2/1/2021

2. Controls related to access and change management could be improved.

Recommendations:

The Police Chief should require TSD to:

A. Work with other Police Department units to establish policies and procedures to ensure timely deactivation of separated employees' access and centralize user access information, including authorizations to add, change, or remove user access.

B. Review existing access to department server rooms and restrict access on a least-privilege basis.

C. Establish policies and procedures for change management, including authorization, documentation and verification of program changes.

MANAGEMENT RESPONSE: Agree

PROPOSED RESOLUTION:

A. A series of formalized process mapping meetings will be scheduled to include multiple departments to capture current process and establish a new structured and improved process.

B. A review of current department server room access will be evaluated and further restricted using a least-privilege principle.

C. A procedure will be put in place to establish policies and procedures for change management, including authorization, documentation and verification of program changes.

RESPONSIBLE PARTY: Director Michael Keran

COMPLETED BY: 2/1/2021

City Auditor's Office
7447 E. Indian School Rd., Suite 205
Scottsdale, Arizona 85251

OFFICE (480) 312-7756
INTEGRITY LINE (480) 312-8348

www.ScottsdaleAZ.gov/auditor

CITY OF SCOTTSDALE

The City Auditor's Office conducts audits to promote operational efficiency, effectiveness, accountability and integrity.