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.