CITY OF SCOTTSDALE

AUDIT HIGHLIGHTS
June 2025

Mark43 Application Controls

Audit No. 2503

WHY WE DID THIS AUDIT

The objective of this audit was to evaluate whether IT general and application controls within the Mark43 application are designed, implemented, and operating effectively to provide reasonable assurance of security, availability, and processing integrity, as well as compliance with related CJIS requirements.

BACKGROUND

We contracted with an independent IT audit consultant, Securance Consulting, to perform this work. The scope of the work covered the Mark43 application and focused on the Records Management System and the Jail Management System modules.

The Scottsdale Police Department (SPD) utilizes Mark43, a cloud-based Software as a Service (SaaS) platform that provides public safety agencies with integrated solutions for records management, corrections/jail management, and data analytics.

WHAT WE FOUND

Stronger user access controls should be implemented to ensure the security of the Mark43 application and data.

Securance Consulting assessed 20 system controls resulting in 3 findings with related recommendations to improve security of and control over the Mark43 application. Overall, no urgent or critical areas of concern were noted. Specifically, findings related to:

- Use of shared accounts limits the ability to monitor user activity within the system.
- Inadequate controls ensuring separation of duties could increase the risk of inappropriate or unauthorized access to sensitive data.
- Policies and procedures do not include guidance specific to SaaS systems

Detailed findings and recommendations were provided to the SPD and are summarized in this public report due to the potentially sensitive nature of the information.

WHAT WE RECOMMEND

The Police Department should:

- Discontinue the use of the admin shared account.
- Ensure user roles and permissions within Mark43 are evaluated and approved in accordance with the principles of least privileges and separation of duties and document the roles assigned to users based on their job duties. Once established, roles should remain static. In addition, ensure a review of all user roles/rights is performed on a periodic basis to certify access continues to be appropriate based on each user’s current job position or duties.
- Work with the City IT Department to assess risks related to SaaS systems and update existing policies and procedures (AR136 – Networking and Computer Security) to address these risks, including evaluating when a SOC 2 or comparable assessment report of vendor-managed controls should be obtained and reviewed.