CITY AUDITOR'S OFFICE

Mark43 Application Controls

June 20, 2025 AUDIT NO. 2503

June 20, 2025

Honorable Mayor and Members of the City Council:

Enclosed is the audit report for *Mark43 Application Controls,* which was included on the Council-approved FY 2024/25 Audit Plan. This audit was conducted to evaluate whether IT general and application controls are designed, implemented, and operating effectively to provide reasonable assurance of security, availability, and processing integrity, as well as compliance with related CJIS requirements. Our office contracted with an IT audit specialist, Securance Consulting, to perform this work.

Overall, no urgent or critical areas of concern were noted. The audit team made a few recommendations for improvements to governance and access management, such as discontinuing the use of shared administrative accounts and documenting policies for assigning user roles and management's review and approval of those assignments.

We thank the Police Department for their time and assistance with this audit. If you need additional information or have any questions, please contact me at (480) 312-7851.

Sincerely,

Lai Cluff

Lai Cluff, CIA
Acting City Auditor

Audit Team:

Travis Attkisson, CISA – Sr. Auditor

Mark43 Application Controls

Audit No. 2503

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.

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.

TABLE OF CONTENTS

OBJECTIVE

An audit of Mark43 Application Controls was included on the City Council-approved fiscal year (FY) 2024/25 Audit Plan as a contracted audit of a selected Information Technology (IT) system or area. The audit objective was to evaluate whether IT general and application controls are designed, implemented, and operating effectively to provide reasonable assurance of security, availability, and processing integrity, as well as compliance with related Criminal Justice Information Services (CJIS) requirements. We contracted with an independent IT audit consultant, Securance Consulting, to perform this work.

The audit team assessed application-related controls for the Scottsdale Police Department's Mark43 system, comprised of the Records Management System and the Jail Management System modules.

BACKGROUND

The Scottsdale Police Department (SPD) utilizes Mark43 technology, which is 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. The application is administered by SPD's Technology Services Division (TSD).

The Mark43 application was acquired in May of 2021 with application modules for Records Management System (RMS) and Computer Aided Dispatch (CAD). The CAD module was not implemented as the design could not meet SPD's standards, and it was later replaced with the development of a Jail Management System (JMS). The RMS module went live November of 2022, and its primary functions include incident reporting, case management, and evidence management. The JMS module went live April of 2023 and allows officers to book and manage arrestees.

Information System Controls

The SPD is required to maintain a minimum set of security requirements to protect and safeguard criminal justice information. Requirements include, among others, implementing system controls that would apply to the IT environment as a whole (IT General Controls) and controls that would be implemented at the application level (IT Application Controls). These controls complement/enhance each other and include controls over user access, change management, data Integrity and processing, vendor management, etc.

Software as a Service (SaaS): Offers the capability to use the provider's applications running on cloud infrastructure. The applications are accessible from various client devices through a thin client interface, such as a web browser.

SOURCE: Information Systems Audit and Control Association

Mark43 runs on a Software as a Service platform, where some of the required controls are managed by the vendor. It is a cloud-based system, and the vendor is responsible for its service commitments, system requirements, secure cloud storage of the city's data, and disaster recovery.

FINDINGS AND ANALYSIS

1. 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. The results of the audit are given below in Figure 1 and were ranked from 1 - Low Risk (No immediate changes recommended) to 5 – Urgent Risk (Immediate remediation required). The 3 areas with assessment of medium or high risk relate to policies and procedures and user access controls, with changes recommended for use of a shared account, and separation of duties.

Figure 1. Summary of findings by control area and assessed risk levels.

No.	Finding Title	5	4	3	2	1	0
8	Use of Shared Account(s)			✓			
1	IT Governance – Policies and Procedures				✓		
6	User Provisioning – SoD				✓		
2	User Provisioning – Access Request					✓	
3	User Provisioning – Terminations					✓	
4	User Provisioning – Periodic Review					✓	
5	User Provisioning – Role-Based Security					✓	
7	Application Authentication					✓	
9	Application Administrator Accounts					✓	
10	Application Configuration					✓	
11	Application Change Management					✓	
12	Programmer Access to Production					✓	
13	Application Data Backup					✓	
14	Application Data Restoration Testing					✓	
15	Application Disaster Recovery Planning					✓	
16	Application Vendor Support					✓	
17	Technical Security of Platform					✓	
18	Technical Security of APIs					✓	
19	Vendor Management					✓	
20	Data Integrity – Migration and API Ingest					✓	
	Total Findings:	0	0	1	2	17	0

SOURCE: Securance Consulting Mark43 Application Audit Report.

A. Use of shared accounts limits the ability to monitor user activity within the system.

The audit noted one shared account used for system administration purposes. The use of shared accounts by multiple individuals limits the ability to monitor or audit who has used the account at any given time. This can be problematic for tracking who accessed information or made system changes. The Scottsdale Police Technology Services Division (TSD) indicated each of the individuals using the shared account are also assigned a separate individual admin account, which would allow for implementation of controls over logging and log monitoring. To reduce the risk of inappropriate access and allow for

monitoring of specific user activity, TSD should discontinue the use of the shared admin account.

B. **Inadequate controls ensuring separation of duties could increase the risk of inappropriate or unauthorized access to sensitive data.**

During the implementation phase of Mark43, user roles were created and assigned for corresponding features and functionality. However, this process and management's review and approval of the final roles and permissions assignments was not documented. Additionally, a periodic review of users and their assigned roles is not being performed.

Controls should be set up to ensure system roles and permissions are in accordance with the principles of least privileges and separation of duties (see textbox). Establishing an approved role-to-functionality matrix (e.g. approved roles/rights to be assigned to users based on job position) could help ensure users are not granted conflicting roles, and reduce the risk of fraud, error and access to sensitive data.

Least Privilege:
The principle to grant individual users and processes only the minimum accesses to system resources and authorizations required to perform their official duties or function.

Separation of Duties (SoD):
The principle requiring the division of roles and responsibilities so that a single individual cannot subvert a critical process or function.

SOURCE: CJIS Security Policy v.5.9.5

The access roles and permissions assigned to users should also be reviewed on a periodic basis to ensure they continue to be appropriate for the individual's position and responsibilities.

C. Policies and procedures do not include information specific to SaaS systems.

Administrative Regulation 136, *Network and Computer Security,* does not specifically address SaaS systems and has not been reviewed/updated since August 2011. Policy guidance on SaaS systems should address, among other things, session management, and data access restrictions.

Additionally, policies and procedures should also provide guidance on the need to obtain and review third-party assurance reports detailing the effectiveness of security controls, such as a SOC 2 report or comparable audit/assessment reports. Controls managed by a third party (e.g. the vendor) are typically tested through a System and Organization Controls (SOC) audit of the vendor, or similar audit/assessments. These reports are made available to clients detailing the effectiveness of security controls the vendor is responsible for. The City contract requires these types of reports be provided and Mark43 provided their SOC 2 report at our request during the audit, but they had not been obtained previously. For higher criticality systems, the Department should verify the results of these assessments prior to finalizing purchasing contracts, as well as reviewing them periodically thereafter to identify any potential issues.

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.

Recommendations:

The Police Chief should require TSD to

1.1 Discontinue the use of the admin shared account.

1.2 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.

1.3 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.

METHODOLOGY & SCOPE

We contracted with an independent IT audit consultant, Securance Consulting (Securance), to perform an audit of the Scottsdale Police Department Mark43 application. As required by Government Auditing Standards, we evaluated the qualifications and independence of these specialists and documented the nature and scope of the specialist's work, including the objectives and scope of work, intended use of the work to support the audit objectives, the specialist's assumptions and methods used, and the specialist's procedures and findings.

For this assessment, Securance followed guidance based on select CoBIT objectives pertaining to the audit scope and internal proprietary knowledge and procedures.

To achieve the objectives of this engagement, Securance designed a layered approach to understand, document, and assess the security and controls supporting the Mark43 application. To meet the audit objectives, the audit team performed the following procedures:

- Reviewed user guides, and administrative guides supporting the Mark43 application.
- Performed a comprehensive review of policies/procedures, interviews of key application and IT process stakeholders, and tested the operating effectiveness of selected controls using a judgmental sample for the following IT processes:
    - Access Management
    - Backup | Restore
    - Change Management
    - Data Migration Integrity
    - Incident Management
    - Interface Security
    - IT Governance
    - Vendor Management
    - Web Application Security
- Assessed the user provisioning and de-provisioning/termination process and appropriateness of administrative rights and tested user profiles to ensure duties are appropriately segregated.
- Reviewed and placed reliance on 3rd party Type II SOC2 and SOC3 reports conducted over the Mark43 application.

- Assessed and validated configurable application controls.

Audit Standards

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 March to May 2025.

MANAGEMENT ACTION PLAN

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

Priority	Recommendation
High	1.1 Discontinue the use of the admin shared account.
Responsible Party: M. Keran, Director Est. Completion Date: 06/16/2025	**Management Response:** Agree **Proposed Resolution:** Inactivate the shared login for Mark43. Admins will use their individual credentials for all admin tasks.

Priority	Recommendation
Med	1.2 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.
Responsible Party: M. Keran, Director Est. Completion Date: 07/31/2025	**Management Response:** Agree **Proposed Resolution:** Police Technology Services (TSD) will ensure user roles and permissions (Mark43's term "abilities") are evaluated and approved in accordance with the principles of least privileges and separation of duties (which is in alignment with our role structure based on job titles/groups). In addition, TSD will 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.

Priority	Recommendation
Med	1.3 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.
Responsible Party: M. Keran, Director Est. Completion Date: 12/31/2025	**Management Response:** Agree **Proposed Resolution:** Administrative Regulation 136 is authored by City IT, and Police Technology Services is open to providing input. All required SOC 2 or comparable assessment reports of vendor-managed controls will be obtained and reviewed for all SaaS solutions for the PD.

City Auditor's Office

Lai Cluff, Acting City Auditor
Travis Attkisson, Senior Auditor
Elizabeth Brandt, Senior Auditor
Mel Merrill, Senior Auditor
Mandi Bradley, Auditor
Shelby Trimaloff, Exec Asst to City Auditor

Our Mission

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

Scottsdale City Auditor
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