AUDIT HIGHLIGHTS

Identity and Access Management

June 14, 2024 Audit No. 2403

WHY WE DID THIS AUDIT

This Identity and Access Management (IAM) audit was included in the Council-approved fiscal year 2023/24 Audit Plan. The objective of this audit was to evaluate the City's processes and controls over identity and access management.

BACKGROUND

We contracted with an independent IT audit consultant, Protiviti, to perform this work. The scope of the work included an evaluation and assessment of the design and operating effectiveness of controls and processes, including key elements of the IAM lifecycle such as account provisioning, account maintenance, activity monitoring/logging, user roles, entitlements and responsibilities, privileged access, password access, password management, account deprovisioning, user access review and IAM tooling.

IAM is a framework of business processes, policies, and technologies that facilitate the management of digital identities to ensure that users only gain access to data when they have the appropriate credentials. City IT is responsible for providing IAM policy requirements and managing the IAM lifecycle along with departmental IT Tech members and SP3s.

City Auditor's Office

City Auditor 480 312-7851
Integrity Line 480 312-8348
www.ScottsdaleAZ.gov

WHAT WE FOUND

Privileged access accounts appear excessive and controls over access management could be strengthened.

Protiviti identified 12 areas for improvement over identity and access management processes and controls, including 2 critical priority areas:

- Excessive number of privileged user accounts – Excessive administrators may lead to inappropriate exposure of sensitive data, and
- Inconsistent enforcement of multi-factor authentication – Using multi-factor authentication decreases the risk of unauthorized access to city systems.

Other non-critical areas for improvement generally covered establishing city-wide policies around user access, enhancing system logging capabilities and processes over granting, removing, and modifying access rights, and conducting a periodic review of such rights.

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

WHAT WE RECOMMEND

We recommend City IT implement the recommendations identified in the detailed Protiviti report and work with the departments to address specific areas that may impact them.

MANAGEMENT RESPONSE

The department agreed with the recommendations.