CITY AUDITOR'S OFFICE

Identity and Access Management

June 14, 2024 AUDIT NO. 2403

June 14, 2024

Honorable Mayor and Members of the City Council:

Enclosed is the audit report for *Identity and Access Management*, which was included on the Council-approved FY 2023/24 Audit Plan as a contracted information technology audit. This audit was conducted to evaluate the City's processes and controls over identity and access management.

We contracted with an independent IT audit specialist, Protiviti, to perform this work. The audit identified several areas for improvement of identity and access management controls. Two critical priority areas to address relate to excessive number of privileged user accounts and consistent implementation of multi-factor authentication throughout the City.

A separate confidential report detailing the audit observations and related recommendations was provided to the IT department. This information is summarized in the public report due to its sensitive nature.

If you need additional information or have any questions, please contact me at (480) 312-7851.

Sincerely,

Lai Cluff, CIA
Acting City Auditor

Audit Team:

Travis Attkisson, Sr. Auditor

TABLE OF CONTENTS

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.

BACKGROUND

This *Identity and Access Management (IAM)* audit was included in the Council-approved fiscal year 2023/24 Audit Plan as a contracted audit of a selected Information Technology (IT) system or area. The objective of this audit was to evaluate the City's processes and controls over identity and access management. 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 management, account deprovisioning, user access review and IAM tooling.

Identity and Access Management

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 IT has adopted the National Institute of Standards and Technology Cybersecurity framework (NIST CSF) as their IT framework. Figure 1 below provides a summary of the 6 Core functions within NIST CSF. This IAM Audit addressed relevant subcategory controls under the Govern, Protect, Detect, and Respond functions.

The Scottsdale Personnel Partnership Program (SP3) consists of department liaisons who help prepare and submit IT work orders for employee access during on-boarding and termination, among other personnel-related responsibilities.

SOURCE: City of Scottsdale HR Department SharePoint site

Figure 1. NIST Cybersecurity Framework

Govern (GV): Cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.
Identify (ID): The organization's current cybersecurity risks are understood.
Protect (PR): Supports the ability to secure assets to prevent or lower the likelihood and impact of adverse cybersecurity events.
Detect (DE): Possible cybersecurity attacks and compromises are found and analyzed.
Respond (RS): Supports the ability to contain the effects cybersecurity incidents.
Recover (RC): Assets and operations affected by a cybersecurity incident are restored.

SOURCE: National Institute of Standards and Technology, Cybersecurity framework (NIST CSF 2.0).

OBJECTIVES, SCOPE, AND METHODOLOGY

An audit of *Identity and Access Management* was included on the City Council-approved fiscal year (FY) 2023/24 Audit Plan as a contracted audit of a selected Information Technology (IT) system or area. The audit objective was to evaluate the City's processes and controls over identity and access management.

We contracted with an independent IT audit consultant, Protiviti, to perform this work. 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, Protiviti followed guidance from the following standards:

- National Institute of Standards and Technology (NIST), Cybersecurity Framework v.2.0, February 2024.
- National Institute of Standards and Technology (NIST), Special Publication 800-53, revision 5, Security and Privacy Controls for Information Systems and Organizations.
- Center for Internet Security (CIS) Critical Security Controls (CSC) v8.

Protiviti assessed IAM processes and controls that support critical systems within the City of Scottsdale. Using a risk-based approach, 10 city departments were included in the assessment, including Information Technology, Water, Traffic, Court, Police, Finance, Community Services, Legal, Public Works and Planning. Protiviti's approach and methodology included the following:

- Preliminary risk assessments of IAM processes.
- Interviews with key technology personnel from each area to evaluate the design of controls and reviewed related documentation.
- Tested the operating effectiveness of controls, including selecting one or two key applications from each of the departments for review.

Overall, the audit identified several areas that can be improved over the City's Identity and Access Management framework. Two critical areas for improvement were identified related to the excessive number of privileged user accounts and inconsistent implementation of multi-factor authentication throughout the City.

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 February to May 2024.

FINDINGS AND ANALYSIS

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

The IAM audit identified 12 areas for improvement over identity and access management controls, with priority ratings from critical to low as given in Table 1 below. Two critical areas for improvements pertained to components under the Protect function of NIST CSF:

1) *The City has an excessive amount of privileged user accounts* – Privileged accounts allow a user to perform security-relevant or administrative-level functions that ordinary users are not authorized to perform. Excessive administrators may lead to inappropriate exposure of sensitive data.
2) *Multi-factor authentication is not consistently implemented throughout the City* – Multi-factor authentication is the process of verifying that a user, or device, is allowed access to specific systems and data through use of more than one authenticator. Using multi-factor authentication decreases the risk of unauthorized access to city systems.

An Authenticator is something a user possesses to verify their identity. Typical Authentication Methods may include:

- Passwords
- ID badge or crypto key
- Bio-metric scans

SOURCE: Auditor summary from NIST SP 800-53 & 63B Digital Identity Guidelines

Table 1: Summary of Areas for Improvement by Priority and CSF function.

Priority	NIST CSF Functions	No. of Areas for Improvement
Critical	Protect	2
High	Protect	3
Medium	Govern, Protect, Detect, Respond	5
Low	Govern, Protect	2
	Total	12

SOURCE: Summarized from the Protiviti IAM report.

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.

Recommendation:

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

MANAGEMENT ACTION PLAN

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

Recommendation

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

Priority	Management Response and Proposed Resolution
Critical	Agree Management agrees and will undertake a review process to validate the business need for current privileged access accounts. Employees without a legitimate business need for privileged access will have it removed. Employees with a legitimate business need will have their accounts vaulted in an IT Security-approved Privileged Access Management tool, providing further protections for those accounts. Additionally, management will review any service accounts with privileged access and remove any accounts without a legitimate business need for the access. Management will also implement a periodic review process for any remaining privileged access accounts to ensure these accounts are reviewed on an ongoing basis. Lastly, management will implement a role-based access model for key business and IT systems. This model will document the privileges required for each role and the risk-based frequency of entitlement reviews. Finally, management already had planned MFA enhancements underway to expand and strengthen the MFA footprint within the City. Management believes these enhancements will further address the opportunities raised by this report.

Responsible Party:	
Kurt Lieber, Chief Information Security Officer Robert Fisher, Information Technology Director	**Est. Completion Date:** December 20, 2025

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 in City Operations.