Remote Access Audit

Department of Innovation & Technology

OBJECTIVES

This audit was conducted to determine whether effective controls are in place to ensure risks related to remote access to the City's network are minimized and connectivity between the network and remote users is secure.

BACKGROUND

The COVID-19 pandemic created a global shift towards the need for mass remote work capabilities for a prolonged period of time. During this time, the City of Mesa offered remote work options to its employees in order to continue providing services to its residents. Remote work, or teleworking, is defined as an arrangement in which an employee works from a remote location, such as the employee's home or another approved alternative location, other than the employee's designated office building.

To ensure business continuity and the safety of employees while teleworking, the City developed and implemented policies allowing eligible and approved employees to incorporate remote work into their schedules. Management Policy 327, *Teleworking*, established criteria for being eligible to telework as well as requirements that employees are expected to comply with. This includes requiring employees to only use equipment that has been encrypted and meets all of the City's security requirements and security standards while working remotely.

The transition to a hybrid workforce introduces significant security risks. For example, employees may use unsecure networks, such as connecting to a free Wi-Fi network, or use personal devices that lack security controls normally found on City-owned devices. These security risks increase the potential of vulnerabilities that can be exploited by hackers. Therefore, ensuring effective security controls are in place for remote access is important to protect the City's network and sensitive data.

The Department of Information and Technology (DoIT) requires its employees who are connecting remotely to the City's network to use a Virtual Private Network (VPN) client with Multi-Factor Authentication (MFA). A VPN is an encrypted connection over the internet from a device to a network that helps ensure sensitive data is transmitted safely while an MFA is an authentication method that requires users to provide two or more verification factors to gain access to a network resource. Once connected, employees have access to critical applications and data essential for fulfilling their job responsibilities effectively.

SUMMARY OF OBSERVATIONS

1. There are no formal policies and procedures in place for managing remote access virtual private network (VPN).

CONCLUSION

In our opinion, the department has effective controls in place to ensure risks related to remote access to the City's network are minimized and connectivity between the network and remote users is secure. However, the department should develop and implement formal policies and procedures for managing its remote access VPN.

ISSUE AND ACTION PLAN

The department does not have formal policies and procedures for managing remote access VPN.

What We Found

The department is responsible for ensuring security risks are mitigated when allowing employees and third-party contractors remote access to the City's network. However, there are no formal policies and procedures in place for managing remote access VPN.

What It Should Be

Effective IT governance and security management standards, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, mandate that organizations establish formal policies and procedures to ensure consistent, secure, and effective management of VPN services. These policies should outline the following:

- responsibilities
- maintenance schedules
- monitoring practices
- incident response protocols

Why Does It Matter

Without formal policies and procedures in place, there is an increased risk that DoIT may not have controls in place to mitigate security risks related to remote access VPN. In addition, a lack of policies and procedures could result in inefficiencies and inconsistencies of applying security measures among DoIT staff when issues arise.

What We Recommend and Management's Action Plans

Recommendation #1-1: The department should develop and implement policies and procedures for managing remote access VPN that address the following:

- Roles and responsibilities of staff involved in VPN management.
- The process for ensuring its VPN client is secure and undergoes the required scheduled maintenance.
- The process for detecting and responding to VPN-related issues, including establishing an incident response plan for addressing incidents such as VPN security breaches.
- Continuously reviewing and updating its policies and procedures to ensure it appropriately addresses evolving security threats and advances in VPN technology.

Action Plan #1-1:

1. Finalize and publish a VPN & Remote Access Policy and Standard that will incorporate recommendations.

2. Define and document roles and responsibilities of staff involved in VPN management in a Service Catalog.
3. Formalize the existing VPN platform maintenance process as a documented and maintained standard operating procedure (SOP).
4. Formalize a response playbook within the City's internal Security Operations Center specifically for responding to various threat types that target VPN access.
5. Establish and formalize an annual review process of policies, standards, and procedures as part of a wider Cybersecurity Governance Program.

Individual or Position Responsible: Jason Bennett, Chief Information Security Officer

Estimated Completion Date: October 31, 2024

SCOPE

The scope of the audit was the period from January 1, 2022 through December 31, 2022. However, some procedures performed consisted of testing currently active City employees and third-party workers.

METHODOLOGY

To accomplish our objective, we performed the following:

- Interviewed DoIT personnel.
- Reviewed policies and procedures and observed processes to gain an understanding of remote user access, including the process for managing remote access VPN.
- Reviewed employment contracts and background check certification forms for third-party workers.
- Selected a sample of active employees, terminated employees, and third-party workers to ensure remote user access was properly granted, revoked, and monitored.

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.

The City Auditor's office provides audit, consulting, and investigative services to identify and minimize risk, maximize efficiencies, improve internal controls, and strengthen accountability to Mesa's citizens. We serve as an independent resource to City Management and the City Council, to provide them with timely, accurate, and objective information, assurances, and recommendations pertaining to City of Mesa programs and activities.

Audit Team

Ron Doba, Internal Auditor
Michelle Hute, Sr. Internal Auditor

City Auditor

Joseph Lisitano, CPA, CIA

Mesa City Auditor's Office

Phone: 480-644-5059
Email: auditor.info@mesaaz.gov
Website: https://www.mesaaz.gov/government/city-auditor
Copies of our audit reports are available at:
https://www.mesaaz.gov/government/city-auditor/audits