Audit of Network Management

Security Controls

In general, the City has implemented security controls to safeguard its technology network. That being said, it has not established an information technology governance framework or security controls framework to guide these activities.

While processes have been developed to grant, change, and disable access to the network, role-based group access, additional monitoring, and standardized authorization documentation would provide further assurance that all access is appropriate.

Finally, a cybersecurity incident response plan has not been established.

Audit Team

City Auditor
Madison Rorschach, CIA, CGAP

Audit Staff
Neeraj Sama, MBA, MS
Amber Jackson, MBA, CFE
Scott Garcia

Audit at a Glance

Why we did this Audit:

A technology network is a system that allows sharing of data and resources. It is critical for organizations that this network be adequately safeguarded to minimize the risk of operational disruption. This audit was included on the City's fiscal year 2021-22 Audit Plan as approved by the City Council.

What we Recommend:

Recommendations 1, 2, 9, 10, & 12
Adopt formal frameworks and establish plans to guide information technology governance & security activities.

Recommendations 3, 4, 5, 6, & 8
Improve network and data center access granting, changing, and monitoring processes.

Recommendation 7
Consider updating the City's data center fire suppression system.

Recommendations 11, 13 & 14
Enhance cybersecurity training & incident response planning.

What we Found:

This audit generally evaluated the strategies and practices implemented by the City to protect its technology network including its information technology management framework, user account and access management, and network security activities. Our findings are summarized below:

IT Framework. The City has not historically adopted an IT management framework to guide decision-making. Tech Services has begun establishing this framework by creating a strategic plan.

User Account & Access Management. Network user accounts are centrally managed by Tech Services. Single sign on is used for the City's critical applications and multifactor authentication is required for remote access. While generally effective practices have been established to grant & disable user network access, clear approval procedures have not been established for changing access. In addition, role-based access groups have not been defined, increasing the risk that users have inappropriate access.

Network Security Activities. Tech Services has implemented general security controls to protect the City's technology network including firewall protections, semi-automatic patching, email filtering & monitoring, malware defenses, data & application backups. Still, adoption of an information technology security framework would provide staff with clear guidance when implementing security controls.

Technology environment changes are generally managed by Tech Services. Additional testing & monitoring could further ensure changes are effective.

Lastly, the City's cybersecurity awareness program complies with State regulations. However, expansion of this program could increase cybersecurity awareness. The City does not have a general government cybersecurity incident response plan.

Introduction

The Internal Audit Department is responsible for providing: (a) an independent appraisal[1] of City operations to ensure policies and procedures are in place and complied with, inclusive of purchasing and contracting; (b) information that is accurate and reliable; (c) assurance that assets are properly recorded and safeguarded; (d) assurance that risks are identified and minimized; and (e) assurance that resources are used economically and efficiently and that the City's objectives are being achieved.

The Internal Audit Department has completed a performance audit of the City's technology network security controls. 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.

Management Responsibility

City management is responsible for ensuring that resources are managed properly and used in compliance with laws and regulations; programs are achieving their objectives; and services are being provided efficiently, effectively, and economically.

Report Confidentiality

Due to the sensitive nature of technology network security control information, detailed findings from this audit have been omitted from this report as they are considered confidential per Texas Government Code § 552.139. This redacted report has been made available for public use and reference.

The full report will be disseminated on a need to know basis in a confidential manner as authorized by the City of Denton's Chief Technology Officer and City Auditor in accordance with all applicable laws and regulations.

It should be noted that this report is the first phase in an audit project series covering the City's management of its technology network. Phase Two Asset Controls will be published in September 2022.

[1] The City of Denton Internal Auditor's Office is considered structurally independent as defined by generally accepted government auditing standard 3.56.