CITY AUDITOR'S OFFICE

Network Security Audit

May 3, 2021

AUDIT REPORT NO. 2106

May 3, 2021

Honorable Mayor and Members of the City Council:

Enclosed is the audit report for *Network Security Audit*, which was included on the Council-approved FY 2020/21 Audit Plan as a contracted audit of a selected information technology system or area. This audit was conducted to evaluate the effectiveness of the City's network controls. We contracted with Berry Dunn McNeil & Parker, LLC (BerryDunn), to perform this work, which included an information technology governance controls review and a technical vulnerability and configuration assessment.

In its review of IT governance, BerryDunn made recommendations to formalize configuration and security standards and roles and responsibilities between IT and departmental technology groups. Further, they recommended the IT department prioritize the completion and testing of its disaster recovery and business continuity plan, and assess the departmental resources allocated to the security function.

BerryDunn's technical review found no critical issues. We provided a separate confidential report of the results and related recommendations to the IT department. This information is not detailed in this public report due to its sensitive nature. If you need additional information or have any questions, please contact me at (480) 312-7867.

Sincerely,

Sharron Walker

Sharron E. Walker, CPA, CFE, CLEA
City Auditor

Audit Team:

Paul Christiansen, CIA, CPA – Sr. Auditor
Lai Cluff, CIA – Sr. Auditor

TABLE OF CONTENTS

AUDIT HIGHLIGHTS

Network Security Audit

May 3, 2021 Audit Report No. 2106

WHY WE DID THIS AUDIT

The *Network Security Audit* was included on the City Council-approved fiscal year (FY) 2020/21 Audit Plan as a contracted audit of a selected information technology (IT) system or area. This audit's objective was to evaluate the effectiveness of the City's network security controls.

BACKGROUND

We contracted with an independent IT Audit specialist, Berry Dunn McNeil & Parker, LLC (BerryDunn), to perform this work. The scope of this review included external vulnerability scanning and penetration testing, server configuration assessment, and an IT governance controls review.

The Information Technology department manages the City's core infrastructure and network components. Additionally, the larger City departments, such as Scottsdale Water, Police, and Community Services, have department-level technology staff that support day-to-day operations and departmental systems.

City Auditor's Office

City Auditor 480 312-7867
Integrity Line 480 312-8348
www.ScottsdaleAZ.gov

WHAT WE FOUND

IT Governance, Policies and Procedures

The following areas for improvement were identified:

- Standards for configuration and hardening of servers and database environments have not been formalized.
- Roles and responsibilities between IT and department technology groups are not clearly identified in a written document, such as a memorandum of understanding.
- Resources needs assessment should be performed to ensure adequate resources are allocated to manage the City's security needs.
- The disaster recovery and business continuity plan for IT has not yet been completed and tested.

Technical Review

No critical issues were identified. A separate confidential report was provided to the IT department detailing the results, along with recommendations to enhance and mature the security of the City's network and technical assets.

WHAT WE RECOMMEND

The IT department appropriately prioritize and address the IT governance and technical matters detailed in the security assessment.

MANAGEMENT RESPONSE

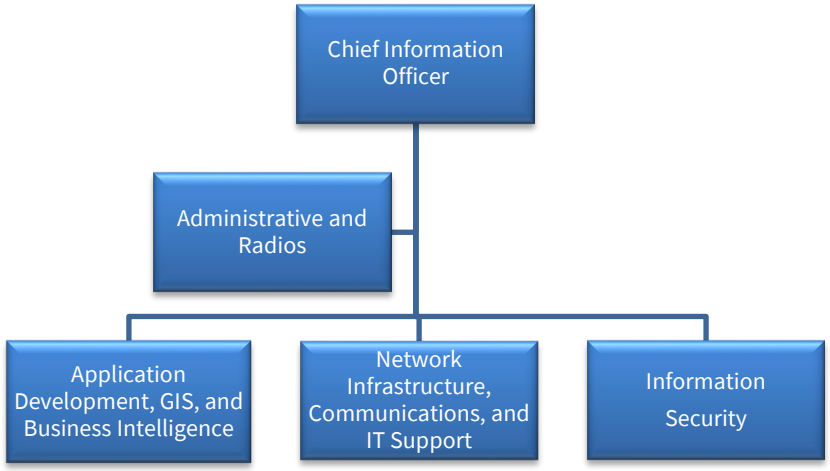
The department agreed with the recommendations and noted that corrective actions are underway.

BACKGROUND

This Network Security Audit was included in the Council-approved fiscal year 2020/21 Audit Plan as a contracted audit of a selected Information Technology (IT) system or area. The objective of this audit was to evaluate the effectiveness of the City's network security controls. We contracted with an independent IT Audit consultant, Berry Dunn McNeil & Parker, LLC (BerryDunn), to perform this work. The scope of this review included external vulnerability scanning and penetration testing, server configuration assessment, and IT governance controls review.

The City's IT department, within the Administrative Services Division, manages the core infrastructure and network components. In fiscal year 2020/21, the department had an authorized personnel budget of 75 full-time equivalent (FTE) positions, organized as illustrated in Figure 1. Additionally, the larger City departments, such as Scottsdale Water, Police, and Community Services, have department-level technology staff that support day-to-day operations and departmental systems.

Figure 1. Information Technology Department Organizational Structure



SOURCE: Auditor analysis of department organizational chart.

BerryDunn performed an administrative review evaluating IT security policies and procedures, and a technical review searching for the City's public network components, conducting vulnerability scanning and penetration testing, and assessing server and database configurations. In searching for all public network components, BerryDunn identified potential targets and using security assessment tools, evaluated and attempted to exploit vulnerabilities.

BerryDunn also selected a sample of the City's approximately 300 servers and databases for configuration assessment. Using a series of tests based on the National Institute of Standards and Technology (NIST) 800-53 controls, the consultant evaluated the existing configuration settings.

OBJECTIVES, SCOPE, AND METHODOLOGY

The *Network Security Audit* was included on the City Council-approved fiscal year (FY) 2020/21 Audit Plan as a contracted audit of a selected information technology (IT) system or area. This audit's objective was to evaluate the effectiveness of the City's network security controls.

We contracted with Berry Dunn McNeil & Parker, LLC (BerryDunn) as the IT audit specialist to perform this review. 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 specialist's work to support the audit objectives, assumptions and methods used by the specialists, and the specialist's procedures and findings.

The audit team, including the City Auditor's office and BerryDunn, interviewed the Chief Information Officer, Chief Information Security Officer, Technology Director, and Director of Applications/GIS to gain an understanding of the department organization and City technology environment. The audit team also interviewed technology staff from Scottsdale Water and the Police Department to learn more about roles and responsibilities relating to their network security management. Using the information gathered, BerryDunn worked with the City Auditor's Office to more specifically define the audit scope and methodology:

- IT governance, policies and procedures review – BerryDunn reviewed enterprise level IT and Security policies and procedures and interviewed IT department management to gain an understanding of key processes.
- External-facing (public) web applications, vulnerability scanning, and penetration testing – BerryDunn conducted discovery scans to identify potential targets for this review. BerryDunn then confirm their validity and reviewed the scanning and testing procedures with the IT department prior to performing the work.
- Server Configuration Assessment – Based on IT and other departments' provided inventory listings of city servers and databases, BerryDunn selected a representative sample of servers and databases for testing. The departments ran BerryDunn-provided configuration assessment scripts and submitted the resulting output for BerryDunn's analysis. This work excluded Scottsdale Water's supervisory control and data acquisition (SCADA) servers and databases, which were undergoing a department-scheduled specialist review.

BerryDunn applied the following standards in its evaluation of security controls:

- National Institute of Standards and Technology (NIST) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.*
- NIST Cybersecurity Framework
- Internal Revenue Service (IRS) Safeguard Computer Security Evaluation Matrix (SCSEM)

The audit's security assessments found no critical issues but made recommendations for strengthening IT governance and 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. Audit work took place from January to March 2021.

FINDINGS AND ANALYSIS

1. IT Governance, Policies and Procedures

BerryDunn reviewed enterprise level information technology (IT) and security policies and procedures. Further, results of their vulnerability scanning, penetration testing and configuration assessment also provided technical context for how these policies and procedures are implemented throughout the City's network infrastructure. The audit identified the following areas where improvements can be made:

A. Standards for configuration and hardening of servers and database environments have not been formalized. Formalized standards can help ensure they are consistently applied throughout the City.

B. Roles and responsibilities between IT and departmental technology groups are not clearly defined. This becomes increasingly important in the event of a security incident or event. Having a clear definition of responsibilities will help reduce the amount of time it takes to respond to an incident.

C. Resources or personnel allocated to the security team may not be adequate to proactively manage the City's security needs. The department should assess its resource needs using a framework or toolkit, such as the *Workforce Framework for Cybersecurity (NICE Framework)* in NIST Special Publication 800-181 or the *Cybersecurity Workforce Development Toolkit* developed by the Department of Homeland Security.[1]

D. The disaster recovery and business continuity (DR/BC) plan for information technology has not yet been completed. Once the DR/BC plan has been developed and approved, the department should run exercises to test the plan. DR/BC plans should be fully exercised and updated on an annual basis to identify any potential issues and to ensure that recovery objectives can be achieved with the planned procedures.

Recommendations:

The IT department should:

A. Formalize configuration and hardening standards for servers and database environments.

B. Create a Memorandum of Understanding (MOU) between the IT department and each of the other City technology groups. The MOUs should clearly define IT and departmental roles and responsibilities to help ensure configuration standards and patching responsibilities are being followed.

C. Perform a resource needs assessment of the IT security function to help ensure it is appropriately resourced and has the required skill sets.

D. Prioritize completion of the disaster recovery business continuity plan and test the plan.

[1] NICE is the National Initiative for Cybersecurity Education.

2. Technical Review

BerryDunn conducted web application scanning, vulnerability scanning, and penetration testing of external-facing (public) components of the City's network infrastructure. They also evaluated configuration settings for servers and databases across various City departments. Though no critical issues were identified, a separate confidential report provided the results along with recommendations to enhance and mature the security of the City's network and technical assets. These detailed findings and recommendations are not detailed in this public report due to the sensitive nature of the information.

Recommendation:

The IT department should appropriately prioritize addressing the matters detailed in the security assessment.

MANAGEMENT ACTION PLAN

1. IT Governance, Policies and Procedures

Recommendations:

The IT department should:

A. Formalize configuration and hardening standards for servers and database environments.

B. Create a Memorandum of Understanding (MOU) between the IT department and each of the other City technology groups. The MOUs should clearly define IT and departmental roles and responsibilities to help ensure configuration standards and patching responsibilities are being followed.

C. Perform a resource needs assessment of the IT security function to help ensure it is appropriately resourced and has the required skill sets.

D. Prioritize completion of the disaster recovery business continuity plan and test the plan.

MANAGEMENT RESPONSE: Agree

PROPOSED RESOLUTION:

A. IT management will produce audit ready documentation of our configuration and hardening standards.

B. While existing documentation and policy are in place, IT will consolidate and formalize an MOU between IT and City Technology groups.

C. An additional headcount is being added in FY 21/22 as part of the Operating Budget. Additional needs for services and headcount will be evaluated once the team is fully staffed (there is currently one vacancy) and the new personnel have been hired.

D. IT management has already made the disaster recovery business continuity plan a priority. The foundational documentation is slated for completion in May 2021 for the recovery of the IT central services required by the City departments. IT will create a plan for tracking testing of those essential services during each fiscal year.

RESPONSIBLE PARTY: Chief Information Security Officer Don Thelander and IT Directors Robert Fisher and Jacob Beard

COMPLETED BY: 12/31/2021

(continued on next page)

2. Technical Review

Recommendation:

The IT department should appropriately prioritize addressing the matters detailed in the security assessment.

MANAGEMENT RESPONSE: Agree

PROPOSED RESOLUTION:

As noted by BerryDunn and the City Auditor, no critical issues were identified. Regardless, IT teams have already corrected one-third of the elements noted. IT teams will continue to correct or planning to correct the areas highlighted by Berry Dunn in their analysis.

Some efforts are not immediately addressable and will require additional funding and staff to address. IT management is preparing requests for the resources required where the items are within scope of IT and will be working with Departments on elements that require their legacy systems to be replaced.

RESPONSIBLE PARTY: IT Directors Jacob Beard and Robert Fisher

COMPLETED BY: 12/31/2022

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 Auditor's Office
Kyla Anderson, Senior Auditor
Paul Christiansen, Senior Auditor
Lai Cluff, Senior Auditor
Brad Hubert, Senior Auditor
Sharron Walker, City Auditor

CITY OF SCOTTSDALE

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