City of Albuquerque

Office of Internal Audit

FOLLOW-UP OF THE
CITYWIDE DATABASE
SECURITY AUDIT
FOLLOW-UP #15-11-103F
June 24, 2015

INTRODUCTION

The Office of Internal Audit (OIA) performed a follow-up of Special Audit No. 11-103, Citywide Database Security. The purpose of this follow-up is to report on the progress made by the Chief Administrative Officer (CAO) and the Information Technology Services Division (ITSD) of the Department of Finance and Administrative Services (DFAS) in addressing our findings and recommendations. Our follow-up procedures rely on the departments providing the status of the recommendations.

Our follow-up is substantially less in scope than an audit. Our objective is to report on the status of corrective actions in regard to our findings and recommendations.

We limited our scope to actions taken to address our audit recommendations from the final audit report dated October 26, 2011, through the submission of actions taken memo completed by the CAO and ITSD dated November 10, 2014, and additional inquiries completed through June 9, 2015.

BACKGROUND

A database is a stored set of related information. Databases contain the information needed by organizations to conduct ongoing business. On a continual basis, organizations must employ information security practices to secure databases from unauthorized access, use, disclosure, disruption, modification, or destruction. The goal of such practices is to provide confidentiality, integrity and availability for information assets.

At the time of the original audit report, the ITSD Database Administrators (DBAs) were maintaining over 300 databases, primarily using Oracle and Standard Query Language (SQL) database management systems. At that time, the City was organized as 23 decentralized departments. Data and information maintained by those departments was also decentralized. A survey of all City departments determined there were approximately 300 databases developed and maintained by City departments, making the Citywide total in excess of 600 databases.

SUMMARY

The audit included four recommendations; three are fully implemented and one is in process. Following the audit, the Administration and DFAS created a new **Sensitive Data** policy, and determined the criticality of business processes through a Business Impact Analysis (BIA). DFAS also implemented a solution for monitoring unauthorized access and created a standardized method for granting and revoking access to the City's databases.

During Fiscal Year (FY) 2015, the Administration adjusted the City's department structure. As a result, the ITSD is transitioning from DFAS to a stand-alone department, the Department of Technology and Innovation. This restructuring will take effect on July 1, 2015. This follow-up retains the wording of the original audit report.

The status of the recommendations is identified by the symbols in the following legend:

🟢 Fully Implemented ⭐ Resolved ◆ In Process 🛑 Not implemented

RECOMMENDATION

The CAO should:

- Develop a City wide policy for the management of sensitive data.
- Ensure the policy is regularly communicated (i.e., New Employee Orientation, City eweb, quarterly communications).
- Regularly remind City users not to store data on the C:\ drive.

RESPONSE FROM THE CAO

"ITSD will develop a city wide policy for the management of sensitive data. Upon the adoption of the policy the City will also create procedures on how this policy will be enforced and how City employees will be notified both initially and on-going."

ESTIMATED COMPLETION DATE

"Policy to be written and promulgated by November 30, 2011."

◆ In Process – DFAS-ITSD created the Sensitive Data policy in 2011. The policy was last revised December 14, 2011 and was approved January 9, 2013. The policy was incorporated in the IT Policies and Standards. The policy is readily available to all City employees. The City's log-on screen reminds employees that they are not to save electronic files and documents on C:\ drives. This recommendation remains in process because the policy is not regularly communicated via channels such as new employee orientation or quarterly communications.

RECOMMENDATION

The CAO should ensure that all City departments are involved in the process of identifying the recovery priority of all City service functions.

RESPONSE FROM THE CAO

"The Administration agrees with the finding.

"ITSD will create a process (through a project plan) to ensure that all City Departments have identified their priority of service functions through a Business Impact Analysis (BIA). A Business Continuity Plan (BCP) will be created for each service function. This will be included in the Enterprise Architecture (EA) Program that is being instituted by ITSD.

"The BCP will be used by ITSD to determine the direction that IT will take for both IT BCP and Disaster Recovery for the City business functions."

ESTIMATED COMPLETION DATE

"Recovery priority project to begin in October 2011 and be completed by March 2012."

● Fully Implemented – DFAS-ITSD conducted a Citywide Business Impact Analysis (BIA) to determine the priority of all City service functions. The BIA and associated business continuity documents involved all City departments and were completed within the estimated completion window.

RECOMMENDATION

DFAS-ITSD should monitor the databases it maintains for unauthorized access.

RESPONSE FROM DFAS

"The department agrees with the finding.

"ITSD will determine a process, toolset, and enable controls to monitor unauthorized access to the City's databases. This will include database monitoring as well as network intrusion detection systems (IDS)."

<u>ESTIMATED COMPLETION DATE</u>

"Project to begin in October 2011 and be completed by February 2012."

● Fully Implemented – DFAS-ITSD has implemented security measures that protect the City's network through network and database monitoring for unauthorized access.

<u>RECOMMENDATION</u>

DFAS-ITSD should ensure that written policies and procedures are in place and followed for the granting and terminating of database access.

<u>RESPONSE FROM DFAS</u>

"The department agrees with the finding.

"ITSD will determine a process and procedure to appropriately provision and de-provision accounts and privileges to the City's databases."

<u>ESTIMATED COMPLETION DATE</u>

"Project to begin in October 2011 and be completed by February 2012."

● Fully Implemented – DFAS-ITSD has created a written procedure and implemented a standard workflow for granting and terminating access to the City's databases. A security management tool has been implemented for the granting and termination of administrative database access. All requests are recorded and tracked through a ticketing system.

Senior Information Systems Auditor

REVIEWED:

Internal Audit Manager

APPROVED:

Debra Yoshimura, CPA, CIA, CGAP, CICA
Director, Office of Internal Audit

APPROVED FOR PUBLICATION**:**

Chairperson, Accountability in
Government Oversight Committee