City of San Antonio

Legislation Details (With Text)

File #:	16-4485
Type:	Staff Briefing - Without Ordinance
	In control: Audit Committee
On agenda:	8/16/2016
Title:	AU16-F07 Follow-Up Audit of Finance Department Payment Card Industry (PCI) Security Governance
Sponsors:	
Indexes:	
Code sections:	
Attachments:	1. AU16-F07 Follow-Up Audit of Finance - Payment Card Industry (PCI) Security Governance

Date	Ver.	Action By	Action	Result

AUDIT COMMITTEE SUMMARY
August 16, 2016
Finance Department PCI DSS Security Governance Process
Report Issued July 11, 2016

Background

In September of 2013, the Office of the City Auditor completed an audit of the Finance Department's (Finance) Payment Card Industry Data Security Standards (PCI DSS) Security Governance. The objective of the audit was to determine if the City had adequate governance procedures and controls over the PCI DSS compliance process.

At that time, Office of the City Auditor concluded that the City did not have adequate governance procedures and controls over the PCI DSS compliance process. The City had begun implementing governance procedures and controls, but they were not yet adequate to ensure full compliance. Control deficiencies were identified relating to the: 1) assignment of overall responsibility for the compliance process, 2) lack of a complete listing of personnel and payment solutions in use, 3) monitoring of departments accepting payment cards, and 4) lack of formal policies and training to establish guidelines.

Follow-up Audit Objective

Determine if Finance effectively implemented action plans in response to recommendations in our report issued September 2013.

Audit Scope & Methodology

The audit scope was limited to the recommendations and corrective action plans made in the original report for the period of October 2013 through December 2015.

Audit Conclusions

We determined that Finance has made progress implementing management action plans to address prior audit recommendations. In total, there were four recommendations made to the Finance Department. Two of four action plans have been successfully implemented in response to our recommendations while two are still in progress. Specifically, the Finance Department is in the process of fully implementing the overall assignment of responsibility for PCI DSS compliance and developing formal policies and training for the appropriate handling of payment card information.

We made specific recommendations to address these issues. The Director of Finance concurred with our recommendations and developed a positive corrective action plan.