CITY OF SAN ANTONIO

OFFICE OF THE CITY AUDITOR

Follow-Up Audit of Finance Department

Payment Card Industry (PCI) Security Governance

Project No. AU16-F07

July 11, 2016

Kevin W. Barthold, CPA, CIA, CISA
City Auditor

Executive Summary

As part of our annual Audit Plan approved by City Council, we conducted a follow-up audit of the recommendations made in the Audit of the Finance Department (Finance) Payment Card Industry Data Security Standards (PCI DSS) Security Governance audit report dated September 16, 2013. The objective for this follow-up audit is:

Determine if prior audit recommendations are successfully implemented and working as intended.

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 the action plans have been successfully implemented while the remaining two action plans are still in progress. Specifically, the Finance Department is in the process of fully implementing:

- The overall assignment of responsibility for PCI DSS compliance
- Formal policies and training for the appropriate handling of payment card information

Finance management's verbatim response is in **Appendix B** on page 7.

Table of Contents

Executive Summary i

Background 1

Audit Scope and Methodology 2

Prior Audit Recommendations and Status 3

A. Overall Responsibility for PCI DSS Compliance 3

B. Inventory of Payment Card Systems and Personnel 4

C. Monitoring of Departments Accepting Payment Cards 4

D. Formal Policies and Training for the Acceptance of Payment Cards 5

Appendix A – Staff Acknowledgement 6

Appendix B – Management Response 7

Background

In September of 2013, the Office of the City Auditor completed an audit of the Finance Department's Payment Card Industry Data Security Standards (PCI DSS) Security Governance. The objective of the audit was as follows:

Determine if the City has adequate governance procedures and controls over the PCI DSS process.

The Office of the City Auditor concluded that the City did not have adequate governance procedures and controls over the PCI DSS process. The City had begun implementing governance procedures and controls, but they were not yet adequate to ensure City-wide compliance with PCI DSS, as summarized below:

- Overall responsibility for PCI DSS Compliance had not been assigned.
- No executive officer had been designated to be responsible for the results of self-assessments.
- No complete list existed of personnel and payment equipment/solutions in use within the City, which impeded the monitoring process.
- Not all departments accepting payment cards received the same level of monitoring.
- Expectations were not completely defined and were not formally communicated to the affected personnel.

Finance management agreed with the conclusions and developed action plans to address the audit recommendations.

Audit Scope and Methodology

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

The audit methodology consisted of interviewing personnel from the Finance Department (Finance) and Information Technology Services Department (ITSD) to gain an understanding of newly implemented controls. We reviewed source documents such as policies and procedures, Compliance and Resolution Group reviews and schedule, Administrative Directives (ADs), inventories of user departments, and equipment/solutions for accepting payment cards. We also reviewed Self Assessment Questionnaires (SAQs) completed by ITSD as a part of the PCI DSS compliance process and other requirements promulgated by the PCI Security Standards Council.

We utilized transaction data from the City's SAP accounting system to validate the inventory of departments accepting payment cards. We do not believe that the absence of testing SAP general and application controls had an effect on the results of our audit.

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.

Prior Audit Recommendations and Status

A. Overall Responsibility for PCI DSS Compliance

Prior Recommendations:

- The Finance Director should be assigned ultimate responsibility for compliance with PCI DSS, as it is a process to ensure the security of payments made to the city.

- While ITSD has taken the lead in facilitating the self-assessment process, the directors of ITSD and Finance should sign each self-assessment. Additionally, the director of any user department to which the self-assessment is applicable should sign the self-assessment. This will raise awareness and in turn increase the level of governance over the payment card process.

Status: Partially Implemented

Directors of both Finance and ITSD have assumed responsibility for PCI DSS Compliance, evident by their signatures on the PCI DSS compliance report documentation (SAQs and internal SAQ Executive Summary Reports).

However, the signatures of user department directors to which the self-assessments are applicable were not always found within PCI DSS compliance report documentation. Finance and ITSD have begun providing a summary of the SAQ results in the form of a cover letter which other department directors can add their signature, indicating responsibility for PCI DSS compliance within their departments. However, for COSA's 2014 SAQ that covered traditional payment card swipe terminals, which are used by many departments, none of the directors of the departments using the swipe terminals were asked to sign. The purpose of requiring department director signatures is to increase accountability and awareness about the importance of PCI DSS Compliance.

Updated Recommendation

The Finance Director should require all user department directors to review and sign the internal SAQ Executive Summary for each SAQ that is applicable to their department. This action would increase accountability and awareness of user department responsibility to ensure appropriate payment card handling practices are followed in accordance with PCI DSS guidelines.

B. Inventory of Payment Card Systems and Personnel

Prior Recommendation:

> Each year, prior to the annual self-assessment process for PCI DSS compliance, the Finance Director should require all other department directors to complete an inventory of all the personnel involved and methods used in accepting payment cards as well as all the systems, hardware, software, and vendors involved in the process. This inventory process should be developed to meet the needs of both Finance and ITSD.

Status: Implemented

Finance completed an inventory of all personnel involved and methods used in accepting payment cards. We validated the current PCI DSS inventory list maintained by Finance against all payment card transactions extracted from SAP for fiscal year 2015 up to January 11, 2016. We did not identify any area within the City receiving payment cards that had not been accounted for on the PCI DSS Inventory list.

C. Monitoring of Departments Accepting Payment Cards

Prior Recommendation:

> The Finance Department should update its monitoring of the payment process to include all types of payment processes and all departments accepting payments. Monitoring visits could be customized based on the payment types being received by each department as well as by the methods used to accept payments.

Status: Implemented

Finance updated its monitoring of the payment process to include all types of payment processes. We verified that Finance has expanded Cash Control Reviews to include departments that only accept payment cards.

We reviewed a sample of Cash Control Reports and determined that the Compliance and Resolution Group adequately documents the methods, payment solutions, and personnel in the designated section of the review checklist. Processes that did not adhere to best practices for handling payment card information were documented and appropriate recommendations were noted in the Cash Control Review report.

D. Formal Policies and Training for the Acceptance of Payment Cards

Prior Recommendation:

> The Finance Director, in cooperation with the ITSD Director, should promulgate a comprehensive administrative directive outlining the responsibilities of each department for payment card security and establishing policies as needed. This administrative directive may reference other existing administrative directives for brevity's sake. Additionally, formal training should be developed and provided to all personnel involved in accepting payment cards and their managers. Formal acknowledgement of the requirements should be obtained annually as a reminder to personnel of their importance.

Status: Partially Implemented

Finance confirmed that formal policies and training have not been implemented to effectively guide user departments in the governance and acceptance of payment cards. Finance has drafted an AD, but this has not been approved and disseminated.

Finance does provide some guidance to departments accepting payment cards, through its network of Department Fiscal Administrators (DFAs). DFAs communicate payment card policy informally to the various user departments.

ITSD has implemented a PCI DSS compliance plan that provides guidance to the ITSD Security Team assisting COSA departments to complete the PCI DSS compliance process. This compliance plan serves as both a form of policy as well as a training guide. It outlines the areas and responsibilities of the IT Security Group in the collaborative process of attaining and maintaining PCI DSS compliance. However, this compliance plan is intended only for providing guidance to ITSD personnel and not the user departments themselves.

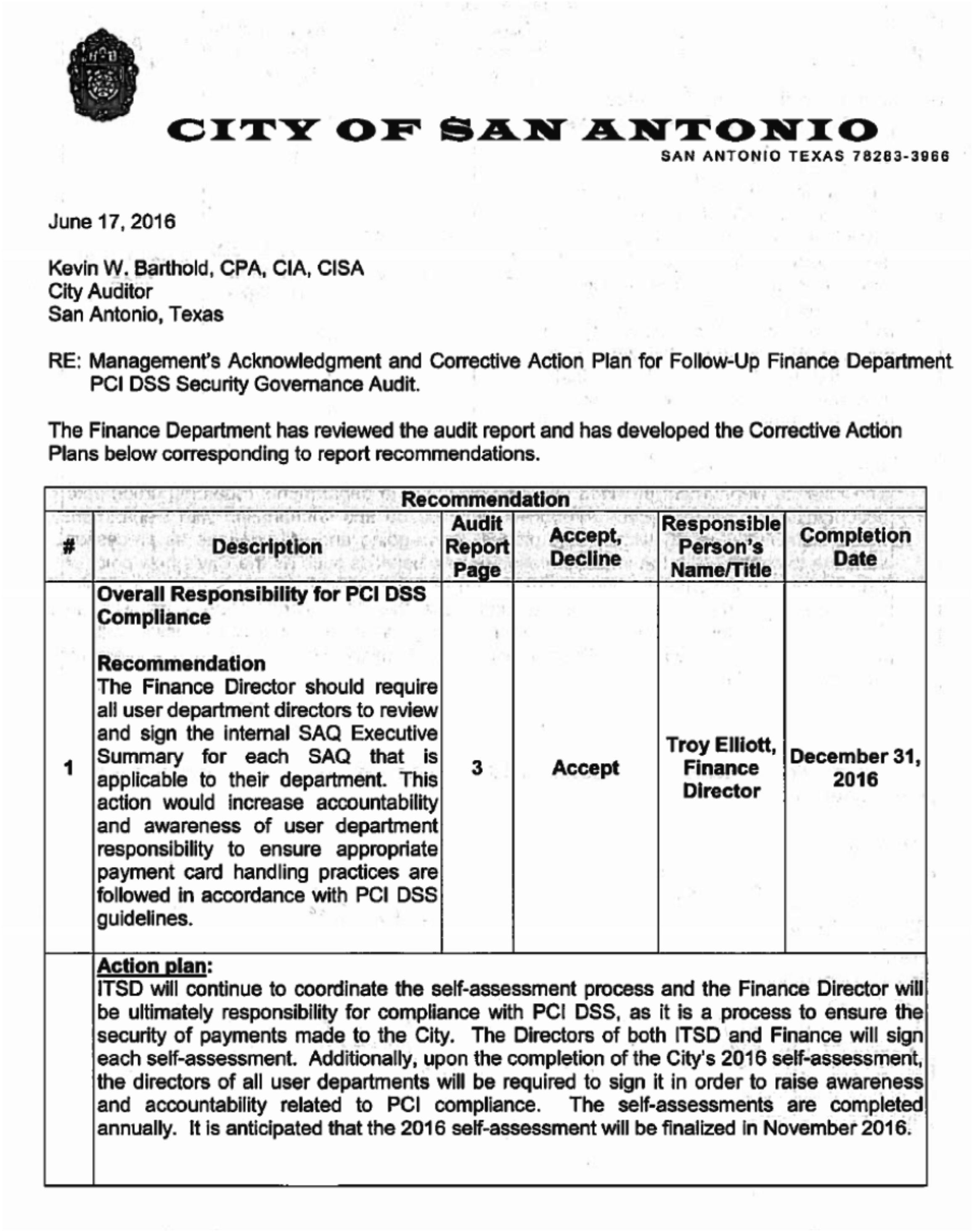
Updated Recommendation

The Finance Director, in cooperation with the ITSD Director, should complete the process of approving and disseminating the draft AD outlining departmental responsibilities for payment card information security. Additionally, formal training based on the new AD should be developed and provided to all personnel and their managers involved in accepting payment cards.

Appendix A – Staff Acknowledgement

Mark Bigler, CPA-Utah, CISA, CFE, Audit Manager
Daniel Kuntzelman, Auditor in Charge
Susan VanHoozer, CISA, CIA, Auditor

Appendix B – Management Response



CITY OF SAN ANTONIO
SAN ANTONIO TEXAS 78283-3966

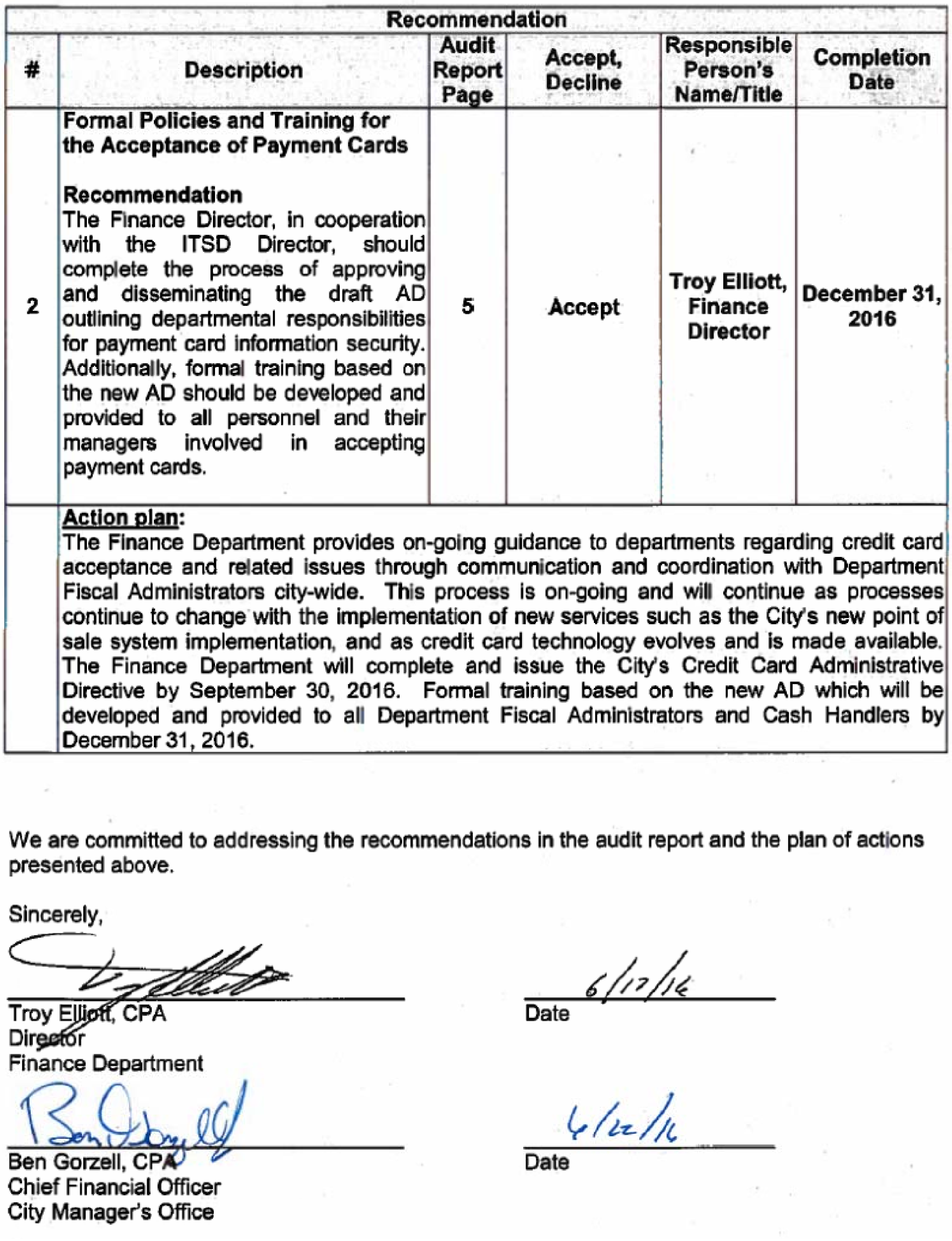
June 17, 2016

Kevin W. Barthold, CPA, CIA, CISA
City Auditor
San Antonio, Texas

RE: Management's Acknowledgment and Corrective Action Plan for Follow-Up Finance Department PCI DSS Security Governance Audit.

The Finance Department has reviewed the audit report and has developed the Corrective Action Plans below corresponding to report recommendations.

Recommendation					
#	Description	Audit Report Page	Accept, Decline	Responsible Person's Name/Title	Completion Date
1	**Overall Responsibility for PCI DSS Compliance** **Recommendation** The Finance Director should require all user department directors to review and sign the internal SAQ Executive Summary for each SAQ that is applicable to their department. This action would increase accountability and awareness of user department responsibility to ensure appropriate payment card handling practices are followed in accordance with PCI DSS guidelines.	3	Accept	Troy Elliott, Finance Director	December 31, 2016
	Action plan: ITSD will continue to coordinate the self-assessment process and the Finance Director will be ultimately responsibility for compliance with PCI DSS, as it is a process to ensure the security of payments made to the City. The Directors of both ITSD and Finance will sign each self-assessment. Additionally, upon the completion of the City's 2016 self-assessment, the directors of all user departments will be required to sign it in order to raise awareness and accountability related to PCI compliance. The self-assessments are completed annually. It is anticipated that the 2016 self-assessment will be finalized in November 2016.				



Recommendation					
#	Description	Audit Report Page	Accept, Decline	Responsible Person's Name/Title	Completion Date
2	**Formal Policies and Training for the Acceptance of Payment Cards** **Recommendation** The Finance Director, in cooperation with the ITSD Director, should complete the process of approving and disseminating the draft AD outlining departmental responsibilities for payment card information security. Additionally, formal training based on the new AD should be developed and provided to all personnel and their managers involved in accepting payment cards.	5	Accept	Troy Elliott, Finance Director	December 31, 2016
	Action plan: The Finance Department provides on-going guidance to departments regarding credit card acceptance and related issues through communication and coordination with Department Fiscal Administrators city-wide. This process is on-going and will continue as processes continue to change with the implementation of new services such as the City's new point of sale system implementation, and as credit card technology evolves and is made available. The Finance Department will complete and issue the City's Credit Card Administrative Directive by September 30, 2016. Formal training based on the new AD which will be developed and provided to all Department Fiscal Administrators and Cash Handlers by December 31, 2016.				

We are committed to addressing the recommendations in the audit report and the plan of actions presented above.

Sincerely,

Troy Elliott, CPA
Director
Finance Department

6/17/16
Date

Ben Gorzell, CPA
Chief Financial Officer
City Manager's Office

6/22/16
Date