



CITY OF SAN ANTONIO

P.O. Box 839966
SAN ANTONIO TEXAS 78283-3966

September 16, 2013

Julián Castro
Mayor

Diego M. Bernal
Councilman, District 1

Ivy R. Taylor
Councilwoman, District 2

Rebecca J. Viagran
Councilwoman, District 3

Rey Saldaña
Councilman, District 4

Shirley Gonzales
Councilwoman, District 5

Ray Lopez
Councilman, District 6

Cris Medina
Councilman, District 7

Ron Nirenberg
Councilman, District 8

Elisa Chan
Councilwoman, District 9

Carlton Soules
Councilman, District 10

SUBJECT: Audit Report of Payment Card Industry Data Security Standards (PCI DSS) Security Governance

Mayor and Council Members:

We are pleased to send you the final report of the Audit of Payment Card Industry Data Security Standards (PCI DSS) Security Governance. This audit began in February 2013 and concluded with an exit meeting with department management in July 2013. Management's verbatim response is included in Appendix B of the report. The Finance Department and Information Technology Services Department management and staff should be commended for their cooperation and assistance during this audit.

The Office of the City Auditor is available to discuss this report with you individually at your convenience.

Respectfully Submitted,

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

Distribution:

Sheryl L. Sculley, City Manager

Ben Gorzell, Chief Financial Officer

Troy Elliott, Director of Finance

Hugh Miller, Director & Chief Technology Officer, ITSD

Michael D. Bernard, City Attorney

Leticia M. Vacek, City Clerk

Robbie Greenblum, Chief of Staff, Office of the Mayor

Jaime Castillo, Communications Director, Office of the Mayor

Frances A. Gonzalez, Assistant to the Mayor, Office of the Mayor

Edward Benavides, Chief of Staff, Office of the City Manager

Donald Crews, Audit Committee Member

Stephen S. Penley, Audit Committee Member

CITY OF SAN ANTONIO
OFFICE OF THE CITY AUDITOR



**Audit of Payment Card Industry Data Security
Standards (PCI DSS) Security Governance**

Project No. AU13-012

September 16, 2013

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

Executive Summary

As part of our annual Audit Plan approved by City Council, we conducted an audit of Payment Card Industry Data Security Standards (PCI DSS) Governance. The audit objectives, conclusions, and recommendations follow:

Does the City have adequate governance procedures and controls over the PCI process? Specifically, has the City:

- ◆ Assigned authority and responsibility for achievement of the PCI DSS requirements,
- ◆ Implemented a reporting and monitoring process for these responsibilities, and
- ◆ Defined expectations for compliance with PCI DSS and formally communicated those expectations to personnel involved in the process?

No, the City does not have adequate governance procedures and controls over the PCI DSS process. The City has begun implementing governance procedures and controls, but they are not yet adequate to ensure City-wide compliance with PCI DSS. We noted:

- ◆ Overall responsibility for PCI compliance has not been assigned.
- ◆ No executive officer is designated to be responsible for the results of self-assessments.
- ◆ There is not a complete list of all personnel and payment equipment/solutions currently in use within the City, which impedes the monitoring process.
- ◆ Not all departments accepting payment cards receive the same level of monitoring.
- ◆ Expectations are not completely defined and are not formally communicated to the affected personnel.

We recommend the City improve governance of the PCI compliance process by:

- ◆ Expressly assigning ultimate responsibility for compliance with PCI DSS to the Director of the Finance Department.
- ◆ Assigning responsibility for signing annual self-assessments to a combination of ITSD, Finance, and other department directors.
- ◆ Conducting regular inventories of personnel accepting payment cards and their processes so that the universe of processes to monitor is known.
- ◆ Ensuring all departments accepting payment cards receive monitoring visits.
- ◆ Promulgating a comprehensive administrative directive for payment security and providing formal training.

ITSD and Finance Management's verbatim responses are in Appendix B.

Table of Contents

Executive Summary	i
Background.....	1
Audit Scope and Methodology	1
Audit Results and Recommendations	2
A. Overall Responsibility for PCI Compliance Has Not Been Assigned	2
B. The Inventory of Payment Card Systems and Personnel with a Role in the Acceptance of Payment Cards is Not Complete	3
C. All Departments Accepting Payment Cards are Not Periodically Monitored.....	4
D. Formal Policies and Training for the Acceptance of Payment Cards Have Not Been Developed	4
Appendix A – Staff Acknowledgement	6
Appendix B – Management Responses	7

Background

The Payment Card Industry Data Security Standard (PCI DSS) is a set of standards for sensitive payment card information. It was developed by the PCI Security Standards Council, which was founded by five global payment brands – American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. Compliance with these standards is mandatory for all merchants (including government organizations) that accept payment cards (credit, debit, and/or gift) from the above brands. PCI DSS standards are designed to help secure payment card information that is stored, processed, or transmitted by merchants. The standards require merchants to either have an annual compliance review or an annual self-assessment of their compliance with the standards.

Currently, multiple City departments have the ability to accept payment cards using a variety of methods. These transactions may take place in person or they may be “card not present” transactions. They may be recorded via a traditional swipe device, using a web site, using an on-line application, taken over the phone, or by using a specialty kiosk (e.g., parking kiosks). The Finance Department acts as the primary intermediary for the City’s contract with the acquiring bank (the bank that processes the City’s payment card transactions).

There are potential penalties for failure to report compliance status in a timely manner as well as for experiencing a breach while not in compliance. A breach of cardholder information can lead to reputational damage, lawsuits, substantial fines and being banned from accepting payment cards.

Audit Scope and Methodology

The audit scope was current processes in place February through March 2013.

We interviewed personnel, reviewed Administrative Directives, departmental policies and procedures, and inventories of departments and equipment/solutions for accepting payment cards, and reviewed requirements and other advice promulgated by the PCI Security Standards Council. We did not utilize data from any information system, and so did not perform any assessment of data reliability or perform general and application controls reviews of any information system

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 Results and Recommendations

A. Overall Responsibility for PCI DSS Compliance Has Not Been Assigned

Executive management has not assigned overall responsibility for ensuring PCI DSS compliance to any individual department. Additionally, no executive manager is currently responsible for signing required annual self-assessments of compliance with PCI standards. These assessments must be signed by an executive officer.

As the acceptance of payment cards is essentially a financial process, the process falls directly under the purview of the Finance Department. However, it does require a multi-disciplinary team to both address and assess compliance.

ITSD has accepted the responsibility of facilitating the annual self-assessment process for all departments, systems, and processes in which the City accepts payment cards (credit cards, PIN-less debit cards, and branded gift cards. However, PCI DSS standards require internal controls that affect not only hardware and software, but also manual internal controls implemented by personnel handling payment card transactions. Thus, every department that accepts payment cards, no matter the means by which it accepts them, has a role in the self-assessment process, as ITSD cannot attest to the behavior of personnel outside of its own department.

Without an executive officer to sign the self-assessments, the City is not compliant with PCI DSS standards, and could incur fines and penalties if a report is required by payment brands or the acquiring bank, and the self-assessment is not provided. Additionally, without executive officer sponsorship, department personnel are less likely to take the security of payment cards as seriously as they should.

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 also sign the self-assessment. This will raise awareness and in turn increase the level of governance over the payment card process.

B. The Inventory of Payment Card Systems and Personnel with a Role in the Acceptance of Payment Cards is Not Complete

ITSD and Finance personnel who are most involved in the PCI compliance process do not have complete information on the personnel conducting payment card transactions or the methods by which they do so.

For example:

- ◆ User department personnel who do not have access to payment acceptance equipment or solutions are accepting payments cards on behalf of the City, writing the card numbers down, and passing that information on to personnel that do have access. This is not well known outside of the user department. Writing card information down raises the risk of non-compliance for the City (because the information may not be protected or disposed of properly), as well as raising the risk of exposure of cardholder data. If the self-assessment does not take this into account because the personnel filling out the self-assessments are unaware of the process, the self-assessment will not be valid, and must be redone.
- ◆ Personnel are accepting payment cards over the phone without the knowledge of the Finance Department, even though Finance department standard operating procedures state that user departments must be authorized to accept phone payments.
- ◆ We identified two payment solutions currently in use by the City that were not on the list used by ITSD to facilitate the self-assessments, because the list was generated by the Finance department for a different purpose. If ITSD is not aware of all outsourced solutions being utilized, it may also not conduct a self-assessment for them, leaving the collection of self-assessments incomplete. IT also cannot help user departments monitor those vendors and solutions for continued compliance, certification, and registration, raising the risk of non-compliance for the City.

Without complete information, policies that are currently being rewritten may not encompass all of the business activities that accept payment cards. Additionally, personnel may not be adequately trained in their responsibilities because ITSD and Finance are not aware that they are accepting payment cards (see Finding D below).

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. The inventory process should be developed to meet the needs of both Finance and ITSD.

C. All Departments Accepting Payment Cards are Not Periodically Monitored

User departments that do not have change funds or petty cash do not receive any monitoring beyond the annual self-assessment of payment card processes (which are currently being completed for the first time). Departments that do handle these types of cash are periodically subject to cash control reviews conducted by Finance's Compliance and Resolution Division. These reviews ensure that Cash Handlers are adhering to applicable rules. If the department being reviewed also accepts payment cards, the reviewer will also check for adherence to best practices for handling payment cards. However, the review is unlikely to include a review of practices of personnel who are not cash-handlers but that accept payment cards.

Since Departments that accept payment cards but that do not accept cash are not getting the same level of monitoring as other departments, they are much more likely to experience a deterioration of operational controls over the payment process.

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.

D. Formal Policies and Training for the Acceptance of Payment Cards Have Not Been Developed

While many administrative directives (both financial and information technology) touch on controls that are essential to ensuring PCI compliance, there is no one directive that summarizes all of the requirements and makes it clear that these controls also apply to the payment card acceptance process. With no administrative directive as a basis, user departments have not developed departmental policies and procedures to support their individual situations and processes as they relate to the acceptance of payment cards.

There is also no formal training regarding the requirements and methods of keeping payment card information secure, other than that for cash handling. Training to-date has been ad-hoc, as personnel interact with Finance and ITSD personnel during a procurement process or self-assessment process. Consequently, personnel that were not involved in these processes will not have received training. Furthermore, rules that Finance has put in place via its internal policies and procedures have not been formally communicated to user departments.

An essential part of the governance of any process is not only the assignment of responsibility, but ensuring that personnel are aware of their responsibilities. This includes ensuring they know what management's expectations are and what the legal and contractual requirements are.

Recommendations

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.

Appendix A – Staff Acknowledgement

Sandra Paiz, CFE, Audit Manager
Susan Van Hoozer, CIA, Auditor in Charge
Christina Liguori, Auditor

Appendix B – Management Responses



CITY OF SAN ANTONIO

SAN ANTONIO TEXAS 78283-3966

July 31, 2013

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

RE: Management's Corrective Action Plan for Audit of Payment Card Industry Data Security Standards (PCI DSS) Security Governance

The Finance Department and the Information Technology Services Department have 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
A	<p>Overall Responsibility for PCI DSS Compliance Has Not Been Assigned</p> <p>◆ 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.</p>	2	Accept	<p>Troy Elliott, Finance Director</p> <p>and</p> <p>Hugh Miller, ITSD Director</p>	December 31, 2013
	<p>◆ 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 also sign the self-assessment. This will raise awareness and in turn increase the level of governance over the payment card process.</p>				

Recommendation					
#	Description	Audit Report Page	Accept, Decline	Responsible Person's Name/Title	Completion Date
	<p>Action plan: ITSD will continue to coordinate the self assessment process and the Finance Director will be assigned ultimate 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 along with the director of any user department in order to raise awareness and accountability related to PCI compliance.</p>				
B	<p>The Inventory of Payment Card Systems and Personnel with a Role in the Acceptance of Payment Cards is Not Complete.</p> <p>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. The inventory process should be developed to meet the needs of both Finance and ITSD.</p>	3	Accept	Margaret U. Villegas, Assistant Finance Director	August 30, 2013
	<p>Action plan: Each year, prior to the annual self-assessment process for PCI DSS compliance, the Finance department will require all departments to complete an inventory of all personnel involved and methods used in accepting payment cards as well as all the systems, hardware, software, and vendors involved in the process and include any outsourced solutions being utilized. The inventory process will be facilitated by Finance and will provide updated information which will be utilized for compliance reviews and targeted training. By August 30, 2013, Finance will update the existing inventory list by requesting updated information and validation from all departments. This inventory list will be coordinated with ITSD and utilized by both departments.</p>				

Recommendation					
#	Description	Audit Report Page	Accept, Decline	Responsible Person's Name/Title	Completion Date
C	<p>All Departments Accepting Payment Cards are Not Periodically Monitored.</p> <p>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.</p>	4	Accept	Dawn Oppermann, Compliance and Resolution Administrator, Finance	Completed
<p>Action plan: In response to the PCI DSS Audit, the Finance Department's Compliance and Resolution Division immediately expanded their cash control reviews to include user departments that do not take cash but do accept credit cards to ensure adherence to best practices for handling credit cards. The Compliance and Resolution Division will further expand their cash control reviews to include compliance with the City's specific requirements for handling credit cards in accordance with the Credit Card Administrative Directive that is scheduled to be completed and issued by September 30, 2013.</p>					

Recommendation					
#	Description	Audit Report Page	Accept, Decline	Responsible Person's Name/Title	Completion Date
D	<p>Formal Policies and Training for the Acceptance of Payment Cards Have Not Been Developed.</p> <ul style="list-style-type: none"> ◆ 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. 	4-5	Accept	Margaret U. Villegas, Assistant Finance Director	September 30, 2013
<p>Action plan: The Finance Department has drafted a comprehensive Administrative Directive for Credit Card acceptance outlining the responsibilities of each department for payment card security and establishing specific policies to guide user departments in their acceptance of credit cards. This new administrative directive will be completed and released by September 30, 2013 in conjunction with training for employees who perform cash and/or credit transactions. Additionally, formal acknowledgement of the requirements will be obtained annually as a reminder to personnel of their importance.</p>					

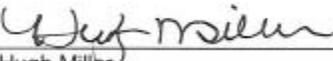
We are committed to addressing the recommendations in the audit report and the plan of actions presented above.

Sincerely,



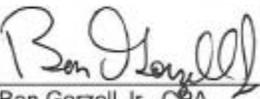
Troy Elliott, CPA
Director
Finance Department

8/01/2013
Date



Hugh Miller
Chief Technology Officer
Information Technology Services Department

08/01/2013
Date



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

8/26/13
Date