Express Memo

PCI Compliance Audit

2021-02
Report Date: 9/28/2020

Background

The City of Glendale accepts payment cards as a form of payment for fees, therefore City departments must adhere to the Payment Card Industry Data Security Standards (PCI DSS) requirements in order to protect customers' cardholder data. Failure to do so may result in significant fines and/or revocation or suspension of payment card processing privileges, increased liability from potential fraudulent charges, and damage to the City's reputation. To ensure compliance with the PCI DSS, the City hired an external Qualified Security Assessor (QSA) to perform an annual assessment. Additionally, in order to assess ongoing compliance with PCI DSS and help City departments better prepare for the annual assessment, Internal Audit is tasked with performing periodic audits of the City's adherence to its PCI Policy (APM 7-9) and departmental Payment Card Acceptance and Processing Procedures (Procedures). The goal is to cover all in-scope sites, systems, and calendar tasks once per year prior to the QSA's annual assessment. This is the second audit of calendar year 2020.

Objective/Scope/Methodology

The objective of this audit is to determine the City's compliance with its PCI Policy and Procedures. The scope of this audit was based upon the PCI DSS in-scope requirements, as defined by the QSA. The detailed scope and methodology are shown in Appendix A.

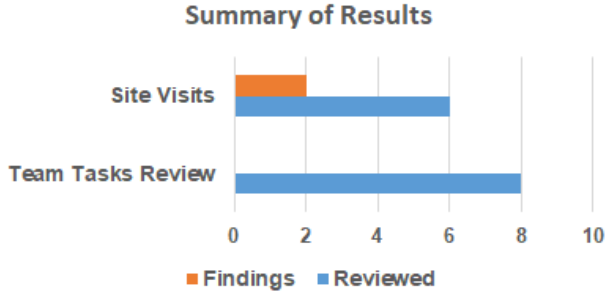
Summary of Results

As of August 31, 2020, there were a total of 55 in-scope sites/systems/tasks, of which 22 were reviewed during the May 2020 audit, 14 were reviewed in this current audit, and 19 are outstanding. Of the 19 outstanding areas, 10 were sites that remained closed as of August 2020 and 9 were calendar tasks that were not due. The table below summarizes the audit status for calendar year 2020.

Calendar Year 2020 Review Status

Column1	May 2020 Audit	Current Audit	Outstanding	Total
Sites	4	6	10	20
Systems	12	0	0	12
Tasks	6	8	9	23
Total	**22**	**14**	**19**	**55**

Based on a review of the 14 areas during this current audit, 2 sites were determined to not be following their departmental Procedures. The table below provides a summary of results based on sites and tasks. The two findings have been remediated. Detailed test results are shown on the next page.



Detailed Results

The table below summarizes the controls and exceptions.

Note 1: All 12 in-scope systems were reviewed in May 2020 and no new systems were identified.

Test	Description	Areas Tested	Findings
1.	Determine if departmental Procedures are being followed through performing site visits.	6	2
2.	Determine if system controls (password policy, user accounts, critical patches) are in place to ensure cardholder data is safeguarded. This includes both testing the hosted system and obtaining compliance documentation from third party vendors that process card payments for the City.	0[1]	0
3.	Determine if the tasks assigned to the PCI Team members are being completed in a timely manner following the Annual PCI Compliance Calendar within the City's PCI DSS Guide.	8	0
Total		**14**	**2**

Findings and Action Taken

The table below details the findings, actions taken, and remediation status.

	Findings	Action Taken
1.	Due to COVID-19, in person card payments have been dramatically reduced. As a result, two departments have been performing tamper seal checks on their payment card terminals (card readers and pin pads) less frequently than what was required per their departmental Procedures.	Staff has agreed to perform tamper seal checks in accordance with their respective departmental PCI procedures. **Status: Remediated**

Distribution List

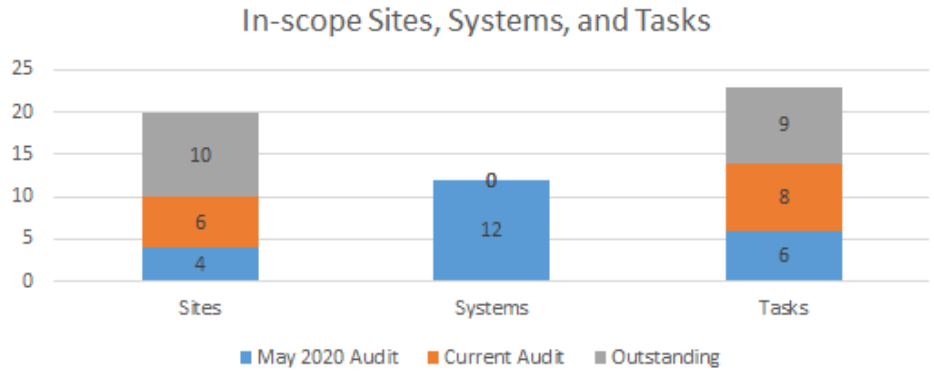
For Action	For Information
• Rafi Manoukian, City Treasurer	• Audit Committee
• Guia Murray, Assistant City Treasurer	• City Council
	• Yasmin K. Beers, City Manager
	• Roubik Golanian, Assistant City Manager
	• Aram Adjemian, City Clerk
	• Elena Bolbolian, Director of Innovation, Performance, & Audit
	• Jason Bradford, Chief Information Officer
	• Onnig Bulanikian, Director of Community Services & Parks
	• Matthew Doyle, Director of Human Resources
	• Yazdan Emrani, Director of Public Works
	• Michele Flynn, Director of Finance
	• Michael J. Garcia, City Attorney
	• Philip Lanzafame, Director of Community Development
	• Silvio Lanzas, Fire Chief
	• Carl Povilaitis, Police Chief
	• Gary Shaffer, Director of Library, Arts & Culture
	• Stephen Zurn, General Manager of Glendale Water & Power

Appendix A: Detailed Scope and Methodology

The City of Glendale processed over 1.7 million payment card transactions in 2019, which makes the City a Level 2 merchant as defined by the PCI Security Standards Council (PCI SSC). To ensure compliance with the PCI DSS, the City hired an external Qualified Security Assessor (QSA) to perform an annual assessment and prepare and submit a formal Report on Compliance (ROC) for the City's required validation. A ROC is required for Level 1 merchant and optional for Level 2.

Scope

The scope of this audit covers the PCI DSS requirements, as defined by the QSA. The in-scope sites, systems, and tasks were based upon the listings maintained by the City Treasurer's Office (CTO). The table below summarizes the testwork performed to date:



Methodology

To gain an understanding of the PCI DSS requirements, Internal Audit shadowed the City's QSA during the 2019 annual PCI audit. Internal Audit also consulted with the QSA and other PCI Team members as needed throughout the audit. Based upon this understanding, the following procedures were developed:

- Review updated Procedures and interview staff to ensure knowledge and compliance of policies and perform the following:
  - Obtain updated device listings from CTO and ensure devices being used are reflected in the device listings.
  - Determine if employees who handle payment card information have taken the necessary PCI training.
- Perform system assessments to ensure third parties have safeguards in place to protect cardholder data. This may involve the following:
  - Collect Attestation of Compliance documents.
  - Review PCI compliance language in City contracts.
  - Perform system reviews.
- Review the City's PCI Policy (APM 7-9) and PCI DSS Guide to ensure:
  - Tasks noted in the Annual PCI Compliance Calendar are being timely performed by assigned parties.
  - Interview PCI Team to determine knowledge and compliance with established roles.

Frequency

Internal Audit plans to test all in-scope sites, systems, and calendar tasks once per year through three separate quarterly audits. The next audit is scheduled to take place in October 2020.