Express Memo

PCI Compliance Audit

City of Glendale
Internal Audit

2022-10
Report Date: 06/29/2022

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 7-8) 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 of three scheduled audits for calendar year 2022.

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.

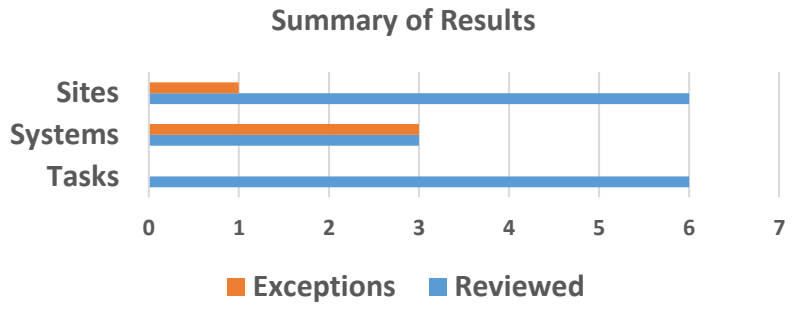
Summary of Results

As of May 31, 2022, there were a total of 56 in-scope sites/systems/tasks, 15 of which were reviewed during the current audit and 17 that are scheduled to be reviewed in the next audit. The table below summarizes the audit schedule for calendar year 2022.

Calendar Year 2022 Audit Schedule

Column1	1st Audit	Current Audit	3rd Audit	Total
Sites	8	6	7	21
Systems	0	3	3	6
Tasks	16	6	7	29
Total	**24**	**15**	**17**	**56**

Based on a review of the 15 areas, 4 exceptions were noted with respects to PCI training and Attestation of Compliance (AOC) forms submitted by third party service providers (TPSP). The PCI training issue was remediated, and the AOC issue is currently being addressed.



Detailed Results

The table below summarizes the controls, number of areas tested, and any exception(s) noted.

Test	Description	Areas Tested	Exception(s)
1.	Determine if departmental Procedures are being followed through performing site visits.	6	1
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 service providers that utilize the City's merchant ID to process payments cards.	3	3
3.	Determine if the calendar tasks assigned to the PCI Team members are being completed in a timely manner per the City's PCI DSS Guide.	6	0
	Total	**15**	**4**

Exceptions and Actions Taken

The table below details the exception(s), action(s) taken, and remediation status.

	Exception(s)	Action(s) Taken
1.	One site had a total of four employees who either processed or could process payment cards without taking the requisite PCI training.	All four employees have completed PCI training. Management has been reminded of the PCI training requirements found within Administrative Policy Manual, Policy 7-8, for all employees who process payment card transactions. **Status: Remediated**
2.	An AOC is a declaration of an organization's compliance with the PCI DSS. It provides evidence that an organization demonstrated adequate controls to secure cardholder data. The City obtains AOCs from all its TPSPs that utilize City Merchant IDs and forwards them to the City's QSA for review and approval. Internal Audit requested the City's current QSA to re-review the AOCs provided by three TPSPs. Although initially approved by the previous QSA, upon re-review, additional recommendations are being made by the current QSA to all three AOCs that require corrections.	The City Treasure's Office (CTO) is currently working with departments and the City's QSA to obtain corrected AOCs from TPSPs. The CTO is also developing a due diligence checklist for City staff to perform preliminary reviews of submitted AOCs. Anticipated completion is September 30, 2022. **Status: In Progress**

Distribution List

For Action	For Information
• Rafi Manoukian, City Treasurer	• Audit Committee
• Guia Murray, Assistant City Treasurer	• City Council
• Onnig Bulanikian, Director of Community Services & Parks	• Aram Adjemian, City Clerk
• Yazdan Emrani, Director of Public Works	• Jason Bradford, Director of Finance & Information Technology
• Silvio Lanzas, Fire Chief & Deputy City Manager	• Michael J. Garcia, City Attorney
	• Roubik Golanian, City Manager
	• Aymee Martin, Interim Director of Human Resources
	• Carl Povilaitis, Police Chief
	• Tamar Sadd, Principle Administrative Officer of Community Development
	• Gary Shaffer, Director of Library, Arts & Culture
	• John Takhtalian, Deputy City Manager
	• Mark Young, General Manager of Glendale Water & Power

Appendix A: Detailed Scope and Methodology

The City of Glendale became a Level 2 merchant (1-6 million transactions) in 2018 based on its number of payment card transactions processed in 2017. For calendar year 2021, the City processed over 722,000 credit card transactions, which is less than the 1 million lower limit threshold. However, Visa, one of the major payment card processing entities, did not recommend changes the City's Merchant Level. Therefore, the City will remain a Level 2 Merchant for 2022.

To ensure compliance with the PCI DSS, the City hired an external 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 is optional for a Level 2 merchant.

Scope

The scope of this audit covers the PCI DSS requirements, as defined by the QSA and documented within the 2022 PCI Audit Plan shared with the PCI Team at beginning of the calendar year. The in-scope sites, systems, and tasks were based upon the listings maintained by the City Treasurer's Office.

Methodology

To gain an understanding of the PCI DSS requirements, Internal Audit shadowed the City's QSA during the 2021 annual PCI audit. Internal Audit also consulted with the QSA and/or 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. This may involve the following:
  - Obtaining updated device listings from CTO and ensure devices being used are reflected in the device listings.
  - Verifying that 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:
  - Collecting Attestation of Compliance documents.
  - Reviewing PCI compliance language in City contracts.
  - Performing system reviews.
- Review the City's PCI Policy (APM 7-8) and PCI DSS Guide to ensure knowledge and compliance of policies. This may involve the following:
  - Reviewing tasks noted in the Annual PCI Compliance Calendar and ensure they are being timely performed by assigned parties.
  - Interviewing PCI Team members to determine their 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 September 2022.