Express Memo

PCI Compliance Audit

City of Glendale
Internal Audit

2024-05
Report Date: 04/30/2024

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 first of three audits scheduled for Calendar Year (CY) 2024.

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.

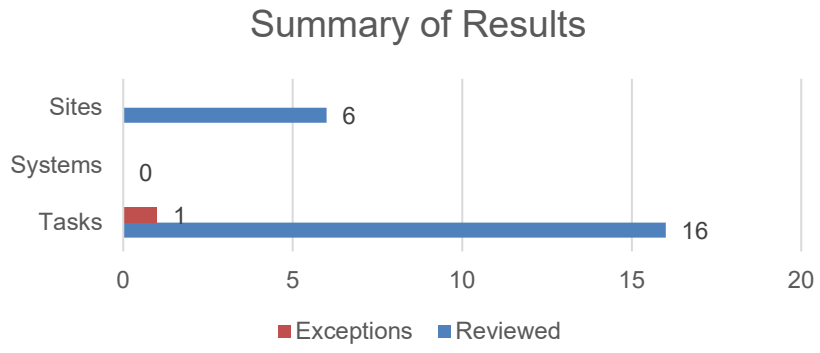
Summary of Results

As of February 29, 2024, there were a total of 53 in-scope sites/systems/tasks, 22 of which were reviewed during the current audit and 31 that are scheduled to be reviewed in future audits. The table below summarizes the audit schedule for CY 2024.

Calendar Year 2024 Audit Schedule

Column1	Current Audit	2nd Audit	3rd Audit	Total
Sites	6	8	5	19
Systems	0	2	3	5
Tasks	16	6	7	29
Total	**22**	**16**	**15**	**53**

Based on a review of the 22 areas, there was one exception noted.



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	0
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 utilize the City's merchant ID to process payments cards.	0	0
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.	16	1
	Total	**22**	**1**

Exceptions and Actions Taken

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

	Exception(s)	Action(s) Taken
1.	Due to the transition of the QSA, there was one Information Technology calendar task that was not completed. This item is a PCI DSS requirement that was determined by the City's QSA to not be within the City's scope, but is performed by the City as a best practice.	The Information Technology Department has now assumed this calendar task and it will be performed on a quarterly basis. **Status: Remediated**

Distribution List

For Action	For Information
• Rafi Manoukian, City Treasurer	• Audit Committee
• Guia Murray, Assistant City Treasurer	• City Council
	• Suzie Abajian, City Clerk
	• Paula Adams, Chief Human Resources Officer
	• Jason Bradford, Director of Finance & Information Technology
	• Onnig Bulanikian, Director of Community Services & Parks and Interim Director of Library, Arts & Culture
	• Bradley Calvert, Director of Community Development
	• Manuel Cid, Police Chief
	• Gregory Fish, Fire Chief
	• Michael J. Garcia, City Attorney
	• Roubik Golanian, City Manager
	• Daniel Hernandez, Interim Director of Public Works
	• John Takhtalian, Assistant 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 CY 2023, the City processed over 826,000 credit card transactions and is currently waiting for the card organization's annual assessment of the PCI DSS merchant level that is currently in progress and anticipated to be received in June 2024.

To ensure compliance with the PCI DSS, the City is in the process of hiring 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 a 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 2024 PCI Audit Plan shared with the PCI Team at beginning of the CY. The in-scope sites, systems, and tasks were based upon the listings maintained by the City Treasurer's Office (CTO).

Methodology

To gain an understanding of the PCI DSS requirements, Internal Audit shadowed the City's QSA during the 2021, 2022, and 2023 annual PCI audits. 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 the 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 ensuring 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 June 2024.