Express Memo

PCI Compliance Audit

City of Glendale
Internal Audit

2025-02
Report Date: 11/01/2024

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 last of three audits scheduled for calendar year 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

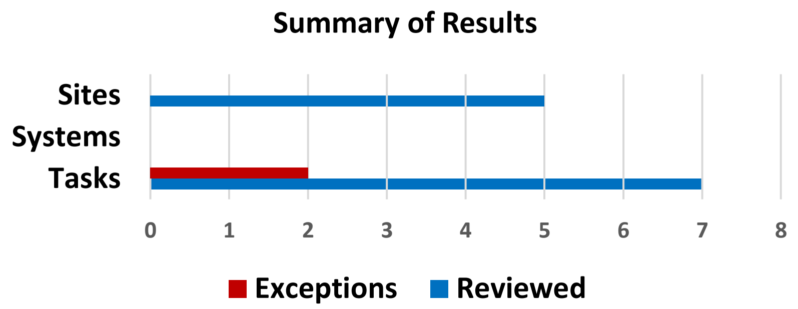
As of August 31, 2024, there were a total of 53 in-scope sites/systems/tasks, 36 of which were previously reviewed, 12 reviewed during the current audit, and 5 system reviews that were deferred pending the QSA's completion of a PCI DSS v4.0 gap analysis. The table below summarizes the audit schedule for calendar year 2024.

Calendar Year 2024 Audit Schedule

	1st Audit	2nd Audit	Current Audit	Total
Sites	6	8	5	19
Systems[1]	0	0	0	0
Tasks	16	6	7	29
Total	**22**	**14**	**12**	**48**

[1] Five system reviews have been removed from the calendar year 2024 audit schedule pending completion of a PCI DSS v4.0 gap analysis by a QSA, a walkthrough of the new PCI DSS v4.0 requirements, and clarification of the evidence necessary to demonstrate the City's compliance.

Based on a review of the 12 areas, there were two exceptions related to the timely completion of calendar tasks.



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.	5	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.	7	2
	Total	**12**	**2**

Exceptions and Actions Taken

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

	Exception(s)	Recommendation(s)
1.	Two calendar tasks related to the following: a. Annual review and/or update of the System Administrative Procedures was not performed timely. b. An expired Service Provider Attestation of Compliance (AOC).	It is recommended that management perform the following in a timely manner: a. Review and/or update the System Administrative Procedures. **Status: In Progress** b. Ensure that new AOCs are received timely and/or require the service provider to comply with the PCI Compliance submit a bridge agreement, a temporary document that allows an organization to continue processing card transactions while it works toward full PCI compliance, explaining the delay in the completion and submission of their current AOC. **Status: Remediated**

Distribution List

For Action	For Information
• Rafi Manoukian, City Treasurer	• Audit Committee
• Jason Bradford, Chief Information Officer	• City Council
• Guia Murray, Assistant City Treasurer	• Suzie Abajian, City Clerk
• Chris Lemus, Cybersecurity Manager	• Paula Adams, Chief Human Resources Officer
	• Onnig Bulanikian, Director of Community Services & Parks
	• Bradley Calvert, Director of Community Development
	• Manuel Cid, Police Chief
	• Daniel Hernandez, Interim Director of Public Works
	• Michele Flynn, Interim Director of Finance
	• Greg Fish, Fire Chief
	• Michael J. Garcia, City Attorney
	• Roubik Golanian, City Manager
	• Lessa Pelayo-Lozada, Acting Director of Library, Arts & Culture
	• John Takhtalian, Assistant City Manager
	• Manuel Robledo, Acting 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 2023, the City processed over 993,500 credit card transactions and received notification from Bank of America that the card organization's annual assessment of the City of Glendale's merchant level has been lowered From PCI DSS Level 2 to PCI DSS Level 3 (20,000–1 million transactions).

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 and 3 merchants.

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 calendar year. 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 2022 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 March 2025.