



PCI Compliance Audit

2025-04

Report Date: 3/31/2025

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 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, 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) 2025.

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 28, 2025, 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 2025.

Calendar Year 2025 Audit Schedule

	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, three sites had exceptions related to the performance of periodic tamper seal reviews and the completion of the requisite PCI training. All exceptions identified were subsequently remediated by the applicable departments.

Summary of Results



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 site visits.	6	3
2.	Determine if system controls (password policy, user accounts, critical patches) are in place to safeguard cardholder data. 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	0
	Total	22	3

Exceptions and Actions Taken

The table below details the exception(s), action(s) taken, and remediation status.¹

	Exception(s)	Action(s) Taken
1.	Two sites did not consistently perform and/or document the required daily tamper seal review.	Department supervisors have reminded staff that they are required to complete and document their tamper review daily. Internal Audit has also provided the existing template on how to complete the tamper seal reviews to affected departments as a reminder. Status: Remediated
2.	Two sites had a total of three employees who either processed or could process payment cards that had not completed the required PCI DSS training.	Department supervisors have been instructed to not allow employees to process credit card transactions until the required PCI DSS Training has been completed. Status: Remediated

¹ The Exceptions and Actions Taken results are presented by exception category and not by the number of unique sites. A single site may be categorized under multiple exceptions.

Distribution List

For Action	For Information
<ul style="list-style-type: none"> Rafi Manoukian, City Treasurer 	<ul style="list-style-type: none"> Audit Committee
<ul style="list-style-type: none"> Guia Murray, Assistant City Treasurer 	<ul style="list-style-type: none"> City Council
	<ul style="list-style-type: none"> Suzie Abajian, City Clerk
	<ul style="list-style-type: none"> Paula Adams, Chief Human Resources Officer
	<ul style="list-style-type: none"> Jason Bradford, Chief Information Officer
	<ul style="list-style-type: none"> Jeffrey Brooks, Acting Fire Chief
	<ul style="list-style-type: none"> Onnig Bulanikian, Director of Community Services and Parks
	<ul style="list-style-type: none"> Bradley Calvert, Director of Community Development
	<ul style="list-style-type: none"> Manuel Cid, Police Chief
	<ul style="list-style-type: none"> Michael J. Garcia, City Attorney
	<ul style="list-style-type: none"> Roubik Golanian, City Manager
	<ul style="list-style-type: none"> Daniel Hernandez, Director of Public Works
	<ul style="list-style-type: none"> Chris Lemus, Cybersecurity Manager
	<ul style="list-style-type: none"> Scott Mellon, Acting General Manager of Glendale Water & Power
	<ul style="list-style-type: none"> Jason Miller, Assistant Chief Information Officer - Infrastructure
	<ul style="list-style-type: none"> Lessa Pelayo-Lozada, Director of Library, Arts & Culture
	<ul style="list-style-type: none"> John Takhtalian, Assistant City Manager/Interim Director of Finance

Appendix A: Detailed Scope and Methodology

As of June 10, 2024, the City of Glendale's merchant level was re-assessed from a Level 2 merchant (1-6 million transactions) to a Level 3 merchant (20,000-1 million transactions) based on its number of payment card transactions processed in 2023. For CY 2024, the City processed over 845,000 credit card transactions. The City is currently waiting for the card organization's annual assessment of the PCI DSS merchant level that is in progress and anticipated to be received in June 2025.

To ensure PCI DSS compliance, in September 2024, 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. While a Level 3 merchant is required to complete an annual Self-Assessment Questionnaire (SAQ) and submit an Attestation of Compliance (AOC), the City opted to have a ROC, which is only required for a Level 1 merchant, completed by an independent QSA. The ROC, issued on December 18, 2024, provided an overall assessment result of "Compliant" for the City, indicating full compliance with all sections of the PCI DSS requirements.

Scope

The scope of this audit covers the PCI DSS requirements, as defined by the QSA and documented within the 2025 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 has shadowed the City's QSA during each of their annual PCI audits since 2021. 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 2025.