



Annual Credit Card Security Review

Citywide



OBJECTIVES

Our annual credit card security review is an assessment of the City's operational efforts to protect cardholder data and sensitive authentication data, as required by the Payment Card Industry Data Security Standard (PCI DSS).

BACKGROUND


The PCI Data Security Standards are technical and operational requirements developed to protect cardholder data and sensitive authentication data. The standards are administered and managed by the PCI Security Standards Council, whose mission is to enhance payment account data security throughout the transaction process. It applies to all entities that store, process, or transmit cardholder data. This includes those entities that are involved in payment account processing, such as merchants, processors, acquirers, issuers, and service providers.

As a merchant that accepts credit cards as a method of payment, the City is required to comply with PCI DSS requirements. Failure to do so could place customers at risk for fraudulent activity and could result in credit card companies levying fines or prohibiting the City from accepting credit card payments. To help ensure compliance, the Accounting Services Division is responsible for maintaining Management Policy 212, *Credit Card Handling*, and providing training for individuals on PCI DSS requirements and the City's credit card handling policies and procedures. They are also responsible for managing the City's merchant accounts. The Department of Innovation and Technology (DoIT) is responsible for ensuring compliance with the IT-related requirements of PCI DSS as well as the annual submission of a Self-Assessment Questionnaire to the City's acquiring bank.

CONCLUSION

In our opinion, the City had effective controls in place to ensure the operational (non-IT) requirements of PCI DSS were being met and that cardholder data and sensitive authentication data were protected.

Our FY 2023 report included one recommendation, which has been implemented and is summarized in the table below.

Recommendation	Status
1-1: PRCF should implement a control to ensure that all credit card handlers complete training within the required timeframes and that only individuals who have completed the training are processing credit card transactions.	

SCOPE

This review was focused on assessing compliance with the operational (non-IT) requirements of PCI DSS, which apply to the City's credit card acceptance sites. Specific criteria and guidance for assessing compliance were provided by the PCI Security Standards Council's *PCI Data Security Standard Requirements and Testing Procedures v4.0*, March 2022.

METHODOLOGY

To accomplish our objective, we performed the following:

- Interviewed employees to ensure they are aware and knowledgeable of PCI DSS requirements and the City's security policies and procedures.
- Reviewed policies and procedures and observed credit card handling operations and processes to ensure they comply with PCI DSS requirements.
- Reviewed contracts and other documentation to ensure service providers are properly managed.
- Reviewed personnel files and training records to ensure employees who have access to cardholder account data are adequately screened and trained.
- Reviewed DoIT asset inventories and other documentation, such as security evaluations and alerts/notifications, to ensure hardware and software technologies, including custom and bespoke software and wireless access points, are properly managed.

AUDIT STANDARDS

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.



The City Auditor's office provides audit, consulting, and investigative services to identify and minimize risk, maximize efficiencies, improve internal controls, and strengthen accountability to Mesa's citizens. We serve as an independent resource to City Management and the City Council, to provide them with timely, accurate, and objective information, assurances, and recommendations pertaining to City of Mesa programs and activities.

Audit Team

Michelle Hute, Senior Internal Auditor
Ronald Doba, Internal Auditor
Sherry Thomas, Internal Auditor

City Auditor

Joseph Lisitano, CPA, CIA

Mesa City Auditor's Office

Phone: 480-644-5059

Email: auditor.info@mesaaz.gov

Website: <https://www.mesaaz.gov/government/city-auditor>

Copies of our audit reports are available at:

<https://www.mesaaz.gov/government/city-auditor/audits>
