Annual Credit Card Security Review

Citywide

City of Mesa Auditor | March 14, 2023

OBJECTIVES

Our annual credit card security review is an assessment of the City's operational efforts to protect cardholder data, as required by the Payment Card Industry Data Security Standard (PCI DSS). Specifically, our objectives were to determine whether:

- The City maintains and enforces policies and procedures that meet PCI DSS requirements.
- Individuals who handle cardholder data are adequately screened and trained.
- When service providers are used to handle cardholder data, due diligence is performed prior to engaging them, written agreements include required language, and they are monitored annually for PCI DSS compliance.
- Management has implemented corrective action plans in response to prior PCI DSS reviews.

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 card 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 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.

SUMMARY OF OBSERVATIONS

1. Credit card handling training is not always completed within the required timeframes.

CONCLUSION

In our opinion, management has implemented policies and procedures to ensure continued compliance with PCI DSS requirements. However, awareness and compliance with some PCI DSS requirements has not always been consistent. Specifically, ensuring employees complete credit card handling training within PCI DSS timelines is a common recurring issue, often occurring within different departments year to year. For additional details, please see the attached Issue and Action Plan.

Our FY 2022 report included three recommendations, which have been implemented and are summarized in the table below.

Recommendations	Status
1-1: Development Services should implement a control to ensure that all credit card handlers complete training within the required time frames and that only individuals who have completed the training are processing credit card transactions.	✓
1-2: Falcon Field should implement a control to ensure that all credit card handlers complete training within the required time frames and that only individuals who have completed the training are processing credit card transactions.	✓
2-1: To ensure the City's service providers are PCI DSS compliant, Business Services should enforce its written policies and procedures by performing its verification process on its list of service providers at least annually.	✓

ISSUE AND ACTION PLAN #1

Credit card handling training is not always completed within the required timeframes.

What We Found

Six credit card handlers at the Parks, Recreation and Community Facilities (PRCF) Department did not complete their annual credit card handling training while still processing credit card transactions.

What It Should Be

According to PCI DSS v3.2.1, *Requirements and Security Assessment Procedures*, Requirement 12.6.1, the City should educate personnel upon hire and at least annually.

In addition, according to Management Policy 212, *Credit Card Handling*, all personnel involved in the handling of Cardholder Data must obtain a successful background security clearance and shall receive annual training on Credit Card Handling Procedures.

Why Does It Matter

Without proper training, employees may unknowingly mishandle cardholder data, putting customers at risk of credit card fraud.

What We Recommend and Management's Action Plans

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

Action Plan #1-1:
Current: PRCF Information Systems (Info Sys) staff will forward any request for software access that allows for processing financial transactions to PRCF Finance before setting up the users access. PRCF Finance will confirm that user has completed required training, cash and credit card handling, and inform PRCF Info Sys staff that the individual can now be set up to handle financial transactions. PRCF Finance will work with PRCF IS in order to have access to audit users and their primary and secondary user access/permissions.

PRCF keeps a list of credit card handlers which includes when they took their training. On a monthly basis PRCF receives a similar list of card handlers from Financial Services which includes the date of their last training. The Financial Services list is highlighted based on if their training is past due or coming due. PRCF reconciles the list and sends back to Financial Services the list with additions and deletions. PRCF sends an email to the appropriate staff and their supervisor as to their need to take the required training(s). If the training is not taken within the appropriate timeframe, an additional email is sent to PRCF IS stating that the card handler is not permitted to handle financial transactions until the training has been completed and PRCF IS staff is directed to deactivate their access to process financial transactions. The Financial Coordinator will be required to verify that any employees that process financial transactions are up to date on their training(s).

Future: PRCF Finance will be working with PRCF Info Sys to determine the possibility of automating the process which would then send email reminders that their training certifications are about to expire.

Individual or Position Responsible: PRCF Financial Coordinator and Information Systems Coordinator

Estimated Completion Date: Current, March 1, 2023; Future, if feasible, December 31, 2023

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 Security Assessment Procedures v3.2.1*, May 2018.

METHODOLOGY

To accomplish our objective, we performed the following:

- Interviewed staff members 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 cardhandlers are adequately screened and trained.

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.

mesa·az

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