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 and sensitive authentication 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.

SUMMARY OF OBSERVATIONS

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

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. However, controls among various departments should be further improved to ensure employees are aware of and complete the required credit card handling training according to the PCI DSS requirements. For additional details, please see the attached Issue and Action Plan.

ISSUE AND ACTION PLAN

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

What We Found

Seven credit card handlers at Development Services and two credit card handlers at Library Services did not complete their annual credit card handling training while still processing credit card transactions.

One new credit card handler at Business Services did not complete the required credit card handling training within 90 days of beginning their credit card handling responsibilities.

What It Should Be

According to PCI DSS v4.0.1, *Requirements and Testing Procedures*, Requirement 12.6.3, City personnel should receive security awareness training upon hire and at least once every 12 months.

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. In addition, all employees who handle credit card information must take the Credit Card Handling training within 90 days of beginning their credit card handling duties.

Why Does It Matter

Without proper training, employees may unknowingly mishandle cardholder data and/or sensitive authentication data, which puts customers at risk of fraudulent credit card activity.

What We Recommend and Management's Action Plans

Recommendation #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.

Action Plan #1-1: Development Services will utilize iLearnMesa to assign credit card handling training to staff upon hire and then track training progress in iLearnMesa using reports and automated emails. Additionally, supervisors will place calendar reminders on their staff members' calendars to ensure that training is completed in accordance with policy. Additionally, supervisors will also verify that only employees who have completed the required training are authorized to handle credit card transactions.

Individual or Position Responsible: Heather Basford, Deputy Director

Estimated Completion Date: 2/25/2025

Recommendation #1-2: Library 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.

Action Plan #1-2: The department will develop and implement an updated policy and procedure to include the Administrative Support Assistant III (ASA III) monitoring the monthly credit card handling list to monitor staff compliance. In addition, staff will be required to complete the training annually and provide evidence to their direct supervisor and the ASA III and failure by staff to complete the training may result in corrective action and disciplinary measures.

Individual or Position Responsible: ASA III

Estimated Completion Date: 3/27/2025

Recommendation #1-3: Business 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.

Action Plan #1-3: There are approximately 30 staff in Business Services who handle credit cards. This new employee was assigned the training along with the other required training for a new employee in the unit, but she missed this one training. The usual back-up for tracking compliance failed us because the new employee wasn't added yet to the monthly status report from Finance.

As an additional mitigation tool, new employees credit card handling training will be scheduled for employee's first week in the "Week 1 New Hire/Mentor Checklist" and the supervisor will use calendar reminders for both the employee and supervisor to ensure completion. We will continue to use the monthly credit card handling compliance training reports provided by Finance and ensure all new employees are accounted for on the report.

Individual or Position Responsible: Doug Fugate

Estimated Completion Date: 3/1/2025

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 v4.0.1*, June 2024.

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.
- Reviewed network and data-flow diagrams to ensure that accurate diagrams exist that show all connections and account data flows between the City's cardholder data environment and other systems and networks.

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