mesa·az
CITY AUDITOR
mesaaz.gov

20 E Main St Suite 820
PO Box 1466
Mesa, Arizona 85211-1466

AUDIT REPORT **CITY AUDITOR**

Report Date:	**February 23, 2016**
Department:	**Citywide**
Subject:	**Annual Credit Card Security Review**
Lead Auditor:	**Karen Newman**

OBJECTIVES

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

- City departments maintain and enforce policies and procedures that meet PCI DSS requirements.
- Individuals who handle credit card information are adequately screened and trained.
- Management has effectively implemented all corrective action plans developed in response to prior PCI DSS reviews.

SCOPE & METHODOLOGY

This review was focused on assessing compliance with the operational (non-IT) requirements of PCI DSS, which apply to credit card handling activities at the City's 31 credit card acceptance sites. Specific criteria and guidance for assessing compliance were provided by the PCI Security Standards Council's *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures v3.1*, April 2015. To accomplish our objectives, we interviewed staff members; observed operations and processes; and reviewed policies, procedures, document inventories, and training records.

BACKGROUND

As a merchant that accepts credit cards, the City is required to comply with PCI DSS. Failure to do so could place our customers at risk for identity theft and could result in credit card companies levying fines or prohibiting the City from accepting credit card payments. To help ensure compliance citywide, the Accounting Services Division is responsible for maintaining Management Policy 212 – Credit Card Handling (MP 212) and training individuals on PCI DSS requirements and credit card handling procedures. They also manage the City's merchant accounts. The Information Technology Department (ITD) is responsible for ensuring the City's compliance with the IT-related requirements of the PCI DSS.

In April 2015, the PCI DSS was updated to Version 3.1, which provided clarification and guidance, as well as some changes and additional requirements designed to align the Standards with new technologies and emerging threats. For the purpose of this review, some of these new requirements were not fully tested, because updated training had not yet been provided in many departments. These requirements will be more fully tested during next year's review.

CONCLUSION

Prior Year Issues:

Our 2015 report included specific recommendations, which were necessary to ensure continued compliance with PCI DSS requirements. Most of the corrective actions have been implemented, but some were still in progress at the time of this follow-up review. Additional information regarding the status of prior year CAPs is presented in the attached Appendix.

New/Continuing Issues:

Overall, we found that City credit card handling operations are PCI DSS compliant. However, we found two issues that warrant management's attention. Our findings and recommendations are summarized below; and additional details are presented in the attached Corrective Action Plans (CAPs). Since numerous departments are involved in these issues, a complete list of responses is not included in this report. However, all affected departments have been asked to submit responses to the recommendations, and next year's review will include follow-up testing to verify that each of these departments has successfully resolved all outstanding issues.

SUMMARY of FINDINGS & RECOMMENDATIONS

1. We found that 37% of employees who handle credit cards (125 out of 342 citywide) had not attended the required annual training. We are recommending that each department in which employees handle credit cards implement a reliable process to ensure compliance with annual training requirements. Employees and their supervisors should be notified of upcoming due dates for training, and the employees should be required to complete the training on or before their respective due dates.

2. Two departments' written procedures and training materials still do not meet PCI DSS v3.1 requirements related to POS terminals, card swipe/dip devices, and access to Primary Account Numbers (PANs). We are recommending that these departments revise their procedures, as requested by the Accounting Services Division, to include all requirements; and submit them to the Accounting Services Division for approval, as required by Management Policy 212.

CAP #1: Non-compliance with credit card training requirements.

Observation: Many employees who handle credit cards have not attended the required annual training:

Department	Overdue	Total	%
Arts & Culture	40	63	63%
Business Services	11	68	16%
Court	6	28	21%
Development Services	9	10	90%
Falcon Field	0	5	0%
Library	26	49	53%
Police	8	45	18%
PRCF	25	74	34%
Citywide Total	**125**	**342**	**37%**

Comments: PCI DSS requires that credit card handlers be educated upon hire and at least annually regarding the importance of cardholder data security.

Management Policy 212 requires that “all personnel involved in the handling of Cardholder Data shall receive annual training on Credit Card Handling Procedures…” These employees are also required to acknowledge at least annually that they have read and understand the associated policies and procedures.

Management Policy 212 states that “the Accounting Services Division shall be the office of primary responsibility for the development, implementation and continuous improvement of the Credit Card Handling Policy.” The policy also requires them to “approve Department and Division credit card handling procedures” and “Develop and deliver training on PCI DSS requirements and Credit Card Handling Procedures.”

Last year, we recommended that Accounting Services track compliance with credit card training requirements and ensure employees and supervisors are notified when they are due for annual training. In addition, we recommended that a communication plan be implemented to help ensure information regarding available training reaches those who need it.

In response to last year’s recommendations, the Accounting Services Division noted several ways in which they planned to improve this process. Unfortunately, while there have been some improvements made to the training itself, the process for notifying employees that they are due for training has not improved. As a result, compliance levels have dropped citywide.

Recommendation:

1-1. Departments with employees who handle credit cards should implement a reliable process to ensure they maintain compliance with the training requirements of Management Policy 212.

1-2. Accounting Services should track compliance with credit card training requirements and should implement a reliable process to ensure employees and supervisors are notified when they are due for annual training.

CAP #2: Procedures and training materials require updates.

Observation: Departmental procedures and/or training materials at the Libraries and Municipal Court as of December 2015 do not meet PCI DSS v3.1 requirements.

Comments: PCI DSS v3.1 includes new requirements related to procedures and training content for locations that utilize Point of Sale (POS) terminals and/or card swipe/dip devices to gather cardholder data during sales transactions. The requirements also state that procedures must include a list of roles that need access to displays of full Primary Account Numbers along with the business need for such access.

Accounting Services provided the new requirements to these departments and requested that they update their procedures; however, as of the date of this review, these departments had not done so.

Recommendation:

2-1. Library Services and Municipal Court should incorporate the new POS terminal and card swipe/dip device requirements into their procedures and should submit the updated procedures to the Accounting Services Division for approval, as required by Management Policy 212.

2-2. Municipal Court should include in their procedures a list of roles that need access to displays of full Primary Account Numbers (PANs) along with the business need for such access. The PAN masking requirements should also be included.

APPENDIX / CAP IMPLEMENTATION STATUS REPORT

✓ = Implemented ◆ = In Progress x = Not Implemented

2015 Recommendations & Responses	Implementation Status	
CAP #1: Non-compliance with credit card training requirements.		
Recommendation: Accounting Services should track compliance with credit card training requirements and ensure employees and supervisors are notified when they are due for annual training. We recommend that the Learning Center system be used to accomplish this. In addition, a communication plan should be implemented to help ensure information on available training reaches those who need it. **Management Response**: Learning Center does not have the capability to track or notify individual employees of upcoming training requirements or training completion dates. Accounting Services had been in contact with ITD and working with ITD prior to this audit to modify the Learning Center to facilitate this, however this is still a work in progress and ITD is actively working this project. We would anticipate this project being completed by end of fiscal year 2015. In the interim, Accounting Services will track CC Handling training requirement due dates manually and manually notify employees of upcoming CC Handling Training due dates. Employees were notified of available CC Handling Training via "Featured" postings on the Learning Center which gave notice of live CC Handling classes and were often notified directly via email or phone call. Notification generally made approximately 2-3 weeks prior to a training session. Going forward, in addition to continued use of a "Featured" posting on Learning Center, Accounting Services will send email notifications/reminders to all department Fiscal Analyst so that they can notify their members of upcoming training and / or due dates for recurring training requirements. To further assist with tracking and formalize the designation of citywide Credit Card Handlers, as a process does not currently exist, Accounting Service is implementing a Credit Card Handler registration process whereby departments will be required to	**In Progress** Changes are still being made to the Credit Card Handling Training process to ensure that employees are trained per the requirements. A reliable notification process has not been established; therefore, many employees have not met the credit card training requirements.	◆

✓ = Implemented ◆ = In Progress x = Not Implemented

2015 Recommendations & Responses	**Implementation Status**	
complete a Credit Card Handler registration form listing designated Credit Card handlers. This Form will also incorporate an acknowledgement of card handler training requirements and understanding of City Policy and Procedure. Form will require card handler manager's signature.		
CAP #2: Procedures and training materials do not meet PCI DSS v3.0 requirements.		
Recommendation 2-1: Accounting Services should revise the "CC101 Minimum Required Credit Card Handling Procedures" and related training materials to include the new PCI DSS requirements related to tampering and substitution inspections on POS terminal and card swipe/dip devices. The new requirements should be disseminated to all personnel with a need to know. **Management Response**: "CC101 Minimum Required Credit Card Handling Procedures" have been updated to include the new PCI DDS requirements. These will be distributed at upcoming live training sessions, emailed to current credit card handlers, and a notification posted on Inside Mesa regarding revised Credit Card Handling Procedures.	**Implemented** The "CC101 Minimum Required Credit Card Handling Procedures" have been updated to include the new requirements related to tampering.	✓
Recommendation 2-2: Accounting Services should ensure that departmental credit card handling procedures are updated as follows: • Arts & Culture, Library Services, Materials & Supply, Municipal Court, Police and PRCF should incorporate into their procedures the new POS terminal and card swipe/dip device requirements. • Municipal Court and Tax Audit & Collections should include in their procedures a list of roles that need access to displays of full Primary Account Numbers (PANs) along with the business need for such access. The PAN masking requirements should also be included. **Management Response**: Accounting Services will provide all departments with updated Minimum Required Credit Card Handling Procedures, which include the PCI DSS v3.0 revisions,	**In Progress** Arts & Culture, Materials & Supply, Police, Tax Audit & Collections and PRCF have updated their policies and procedures to include the necessary requirements. However, Library Services and the Municipal Court still need to include the new POS terminal and card swipe/dip device requirements; and the Municipal Court also needs to include a list of roles that need access to	◆

✓ = Implemented ◆ = In Progress x = Not Implemented

2015 Recommendations & Responses	**Implementation Status**	
and request that all departments update their procedures accordingly and then submit their revised procedures to Accounting Services for review and approval. The referenced departments above will be included in the process.	displays of full Primary Account Numbers (PANs) along with the business need for such access.	
CAP #3: Service provider contract should require PCI compliance.		
Recommendation 3-1: The department should partner with Purchasing to ensure that this agreement is not renewed unless it is amended to incorporate the PCI DSS requirements. **Management Response**: The vendor has provided the COM with documentation that shows proof of PCI compliance. When we renew or seek proposals in the future all contractual language will include the requirement for PCI compliance.	**Implemented** The RFP developed for the new contract requires PCI DSS compliance.	✓
Recommendation 3-2: City staff should document which PCI DSS requirements are managed by the vendor and should implement a process to monitor the vendor's PCI DSS compliance status. **Management Response**: The City's contract administrator is developing a process to ensure that applicable vendors certify that they are PCI DSS compliant.	**Implemented** The City's Contracts Administrator has implemented a Compliance Policy to ensure that applicable vendors certify that they are PCI DSS compliant.	✓