mesa·az
CITY AUDITOR

mesaaz.gov

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

Date:	March 26, 2015
To:	Audit, Finance and Enterprise Committee
From:	Jennifer Ruttman, City Auditor
Subject:	Annual Credit Card Security Review
cc:	Mayor and Council Michael Kennington, CFO Alex Deshuk, Manager of Technology and Innovation Natalie Lewis, Assistant to the City Manager Ed Quedens, Business Services Department Director Cindy Ornstein, Arts & Culture Department Director

Pursuant to the Council-approved Audit Plan, the City Auditor's office has completed our annual credit card security review, which includes a follow-up review of the prior year's findings. The report is attached will be presented at the next scheduled meeting of the Audit, Finance & Enterprise Committee.

Please feel free to contact me with any questions or concerns.

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:	**March 26, 2015**
Department:	**Citywide**
Subject:	**Annual Credit Card Security Review**
Lead Auditor:	**Dawn von Epp**

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 v3.0*, November 2013. 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 November 2013, the PCI DSS was updated to Version 3.0, which provided clarification and guidance, as well as some changes and additional requirements designed to align the Standards with new technologies and emerging threats. Under Version 3.0, several new requirements are referred to as "best practice until June 30, 2015, after which it becomes a requirement". New requirements related to operations (non-IT) were incorporated into this year's review, to assess the City's readiness to maintain compliance beyond July 1, 2015.

Our 2014 report included specific recommendations for three departments, along with a general recommendation for the City Manager's office to clearly communicate to all departments the need for, and expectation of, ongoing PCI DSS compliance in the future.

CONCLUSION

Follow-up Review:

In our opinion, all of the outstanding corrective actions plans from our prior reviews have been implemented. For additional details, please see the attached APPENDIX.

Current Review:

Overall, we found that City credit card handling operations are in compliance with PCI DSS. However, over the past year, compliance with annual credit card training requirements has dropped significantly. Only 20% of personnel who handle credit cards completed the required training in 2014, down from approximately 91% in 2013. In addition, citywide and departmental policies, procedures, and credit card handling training materials need to be updated to comply with PCI DSS v3.0 requirements related to Point of Sale (POS) terminals and card swipe/dip devices. A summary of our findings and recommendations is included below. For additional details, along with responses from management, please see the attached Corrective Action Plans (CAPs).

SUMMARY of FINDINGS & RECOMMENDATIONS

1. Many employees who handle credit cards have not attended the required annual training. We are recommending that the Accounting Services Division utilize the Learning Center system to track compliance with training requirements and ensure employees and supervisors are notified when they are due for annual training.

2. Citywide and departmental procedures and training materials do not meet PCI DSS v3.0 requirements related to POS terminals, card swipe/dip devices, and access to Primary Account Numbers (PANs). We are recommending that the Accounting

Services Division revise the citywide procedures and training documents and ensure that impacted departments revise their procedures to include the new requirements.

3. One department has a service agreement that involves vendor access to cardholder data but the agreement does not require the vendor to be PCI compliant. We are recommending that this agreement not be renewed unless it is amended to include the requirements, and that the department should partner with Purchasing to ensure that PCI DSS requirements are incorporated into all agreements. In addition, to fully comply with PCI DSS v3.0, staff should implement a process to monitor the service provider's PCI DSS compliance status and should document which requirements are managed by the service provider.

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

Observation:

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

Comments:

PCI DSS requires that applicable personnel be educated upon hire and at least annually regarding the importance of cardholder data security. These employees are also required to acknowledge at least annually that they have read and understand the associated policies and procedures.

From 2013 to 2014, the percentage of credit card handlers that completed required annual training decreased from 91% to 20%.

The drop in compliance appears to be largely due to a change in training delivery systems that resulted in stopping the automated notifications to employees that the annual training was due. Staff also cited as a contributing factor a lack of awareness of when training was being offered.

Recommendation:

1-1. 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:

1-1. Agree.

Implementation Plan:

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 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.

Individual or Position Responsible:
Joseph Scalmato

Estimated Completion Date: 6/30/2015

CAP #2: Procedures and training materials require updates.

Observation: Procedures and training materials do not meet PCI DSS v3.0 requirements.

Comments: PCI DSS v3.0 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. Some requirements became effective 1/1/15 while others do not go into effect until 7/1/15.

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.

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:

2-1. Agree.

Implementation Plan:
"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.

Individual or Position Responsible:
Joseph Scalmato

Estimated Completion Date: 6/30/2015

2-2. Agree.
Implementation Plan:
Accounting Services will provide all departments with updated Minimum Required Credit Card Handling Procedures, which include the PCI DSS v3.0 revisions, 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.

Individual or Position Responsible:
Joseph Scalmato

Estimated Completion Date: 6/30/2015

CAP #3: Service provider contract should require PCI compliance.

Observation:

A service provider contract allows the vendor to have access to customers' cardholder data, but does not require the vendor to be PCI compliant.

Comments:

The City has an agreement with a service provider that does not require that the service provider be responsible for cardholder data security and does not require that they provide evidence of PCI compliance annually. In addition, the vendor is not listed as PCI compliant on the Visa Global Registry of Service Providers, and the vendor's web site does not indicate that they hold any comparable certifications that would mitigate the risk of using a service provider not listed as PCI compliant.

The original 1-year agreement was established in 2006, prior to the City being required to comply with PCI DSS, and has been automatically renewed every year without being amended.

An agreement with a service provider with access to customers' cardholder data should require that the service provider be responsible for cardholder data security and that they provide evidence of PCI compliance annually. In addition, the City is required to document which PCI DSS requirements are managed by the vendor and to have a process in place to monitor the vendor's compliance status. Without these protections, the City is exposed to a higher risk of loss if the vendor does not secure cardholder data.

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.

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:

3-1. Agree.
Implementation Plan:
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.

Estimated Completion Date: 5/1/2015

3-2. Agree.
Implementation Plan:
The City's contract administrator is developing a process to ensure that applicable vendors certify that they are PCI DSS compliant.

Individual or Position Responsible:
Tom LaVell, Contracts Administrator

Estimated Completion Date: 6/30/2015

APPENDIX

Follow-up Review of 2014 CAPs

✓ = Implemented ◆ = In Progress x = Not Implemented

Corrective Action	**Implementation Status**	
i.d.e.a. Museum (formerly AMY)		
Recommendation: AMY should ensure that current fiscal year credit card receipts are secured at all times and that credit card records that exceed the retention schedule are destroyed. In addition, the Friends of AMY credit card terminal should be configured to require a password to process refunds. All credit card terminal passwords should be actively managed to ensure that passwords are known only by employees who need them to perform their job duties, and that passwords are changed periodically, including when there is staff turnover or when the passwords are thought to have been compromised. **Management Response**: *"AMY has secured current year credit card receipts in a locked filing cabinet, and has destroyed all other credit card records. The Friends of AMY credit card terminal is now password protected when a refund is required."*	**Implemented** The i.d.e.a. Museum has appropriately secured current receipts and receipts that were past their retention schedule have been destroyed. All POS terminals are now password protected for processing refunds.	✓
Financial Services, Accounting Services Division		
Recommendation: Accounting Services Division should destroy the numerous credit card documents stored by the City's off-site provider that are now well beyond the retention date. At the time of this review, there were at least 196 cartons known to contain credit card data that were past due for destruction (i.e.	**Implemented** The 196 cartons containing credit card data that were past the retention schedule were destroyed; and a Document Retention Destruction Procedure was	✓

✓= Implemented ◆= In Progress x = Not Implemented

Corrective Action	**Implementation Status**	
more than 7 years old). This has been a finding in all 5 of our PCI DSS reviews; therefore, management should also develop an improved internal control mechanism to ensure compliance with credit card document retention policies in the future. **Management Response**: *"The cartons containing credit card documents have been destroyed. We are currently writing procedures to ensure ongoing compliance with document retention standards."*	developed to ensure future compliance.	
Library Services, Mesa Express Library		
Recommendation: The Mesa Express Library (MEL) should ensure ongoing compliance with departmental credit card handling procedures, which require that: 1. Credit card terminal passwords are changed annually or when there is turnover of staff. 2. Transaction receipts and all other cardholder data, including balancing and audit reports, are secured at all times. **Management Response**: *"The password for MEL's credit card terminal has been reset and will be reset again at least annually. Staff has been trained on all policies and procedures to ensure future compliance. Additionally, Management Policy 210 and 212 as well as Library procedures for cash and credit card handing will be reviewed with all library supervisors annually. Receipts are now stored in a secure location."*	**Implemented** The Mesa Express Library reset the password on the credit card terminal. In approximately July 2014 the terminal was replaced with a terminal that performs both chip and swipe functionality, and which utilizes a password formula which changes daily. Receipts have been appropriately secured.	✓