



AUDIT, FINANCE & ENTERPRISE COMMITTEE

December 8, 2021

The Audit, Finance & Enterprise Committee of the City of Mesa met in the lower-level meeting room of the Council Chambers, 57 East 1st Street, on December 8, 2021, at 4:30 p.m.

COMMITTEE PRESENT	COMMITTEE ABSENT	STAFF PRESENT
Mark Freeman, Chairman Jennifer Duff* David Luna	None	Mike Kennington Dee Ann Mickelsen Bill Taebel

(*Participated in the meeting using video conference equipment.)

Chairman Freeman conducted a roll call.

1. Items from citizens present:

There were no items from citizens present.

2-a. Hear a presentation and discuss the following Audits:

1. Business Services/Purchasing Division – Procurement Processes
2. Fleet Services – Parts Management
3. DoIT – Software/Application Asset Management
4. Engineering – JOC Projects Follow-up Review
5. Annual Credit Card Review

City Auditor Joseph Lisitano displayed a PowerPoint presentation covering three audits, a follow-up review, and the annual credit care review. **(See Attachment 1)**

Mr. Lisitano discussed the Business Services audit was to determine whether effective controls are in place for procurement processes to prevent or detect errors, fraud, waste, or abuse, and ensure compliance with policies, statutes, and other applicable requirements. (See Page 3 of Attachment 1)

Mr. Lisitano stated department staff were interviewed and internal procedures were reviewed to identify and determine the effectiveness of internal controls. He listed the types of purchases that were sampled and tested to ensure the proper procedures were followed. He noted the annual commodity spend review was analyzed to determine whether non-contract purchases could be put onto a contract. (See Page 4 of Attachment 1)

Mr. Lisitano reported the finding that conflicts of interest were not specifically addressed as part of the documented procurement activities. He recommended that existing forms include conflict of interest documentation and that the forms be retained with related files for transparency. (See Page 5 of Attachment 1)

In response to a question from Committeemember Luna, Business Services Department Director Ed Quedens explained the boilerplate Request for Proposal (RFP) identifies any conflicts of interest and there is a long-standing process where each evaluation team member identifies any potential conflict of interest which results in their removal from the evaluation committee. He commented a question regarding conflict of interest has been added to the award recommendation form for those involved in the request for bid.

Mr. Lisitano stated cooperative contract agreements that the City has with other agencies were not always properly approved. He recommended a process be developed to ensure a written agreement is in place prior to using cooperative contracts that confirms the agency's methods are in line with the City's requirements. He advised management agreed with the recommendations and are in the process of implementing the corrective actions, which should be completed by the end of January 2022. (See Pages 6 and 7 of Attachment 1)

Mr. Lisitano mentioned the fleet services audit was to determine whether effective controls are in place over procurement processes to prevent or detect errors, fraud, waste, or abuse, and ensure compliance with policies, statutes, and other applicable requirements. He stated after interviewing staff and reviewing policies and procedures, the audit sampled and tested adjustments to parts inventory, issued parts, and sampled inventory count. He said access to the parts system and warehouse facilities, as well as performance measure goals were reviewed to verify effective controls were in place. (See Pages 8 and 9 of Attachment 1)

Mr. Lisitano outlined the parts management recommendations for following policies and procedures to ensure accurate inventory, restricting physical access to the parts warehouse, creating written policies and procedures for disposing of inactive and obsolete parts, and documenting benchmark criteria measuring performance. (See Pages 10 through 12 of Attachment 1)

Mr. Lisitano advised management agreed with the recommendations and is currently implementing corrective action plans, which should be completed by the end of October 2022. (See Page 13 of Attachment 1)

Responding to a question from Committeemember Luna regarding the process of part disposal, Mr. Quedens stated the options include returning to the vendor for credit, negotiating an exchange, or auction and surplus sale alternatives. He remarked parts rarely go into a garbage dumpster. He mentioned there is a central receiving warehouse in East Mesa where discarded items are housed; however, the store selling the items has been discontinued and the parts are now sold on the Public Surplus website. He added the funding from the sales generally goes back into the General Fund.

In response to a question posed by Chairperson Freeman, Mr. Lisitano advised the departments will typically develop and write their own policies based on the recommendations. He mentioned the Audit Department would assist if needed.

Mr. Lisitano explained the Department of Innovation and Technology (DoIT) audit was performed to determine whether effective controls were in place to ensure all applications used to conduct City business are licensed, inventoried, and meet City IT security standards. (See Page 14 of Attachment 1)

Mr. Lisitano stated the City utilizes many applications and different software from multiple providers and DoIT is responsible for managing and maintaining the applications. He reported out of the 1,400 titles, 279 require license renewals. He said the City implemented a new asset management system and the assets are still being transferred, which has affected the ability to manage the software inventory and licenses. (See Page 15 of Attachment 1)

Mr. Lisitano indicated DoIT staff were interviewed to gain an understanding of department procedures and inventory management, and reviewed policies and procedures to verify that effective controls were in place to ensure applications are licensed, inventoried, and meet security standards. (See Page 16 of Attachment 1)

Mr. Lisitano listed the suggested recommendations to make sure the asset management system used for the inventory of software and applications is accurate and complete. (See Pages 17 and 18 of Attachment 1)

In response to a question from Committeemember Luna regarding whether DoIT has a system to prevent ransomware, Chief Information Officer Travis Cutright stated part of the security team's job is to frequently update the software and operating systems and deploying patches that come out to take care of any vulnerabilities. He pointed out there are firewalls in place and monitors that look for malicious attempts to penetrate the City's network. He provided an example of a recent attempt to hack into the network and because of the City's dual factor authentication the attack was blocked. He reported an IT manager has been assigned to oversee the transfer to the new asset management system which will assist in managing the software.

Mr. Lisitano continued by saying the software and application licenses were not effectively being tracked or monitored and recommended implementing a formal method for tracking. (See Page 19 of Attachment 1)

Responding to an inquiry from Committeemember Luna asking if each department is responsible to make sure the license is up to date, Mr. Lisitano acknowledged that is part of the confusion because there are some licenses that IT tracks but not all.

Mr. Cutright commented that DoIT should be responsible to manage the licenses. He stated most software purchases are routed through DoIT and the ones that are not are usually discovered when a department is attempting installation. He summarized that DoIT is ultimately responsible for updates.

Mr. Lisitano commented that management agreed with the recommendations and the corrective action plans should be completed by December 2022. (See Page 20 of Attachment 1)

In response to a question from Chairperson Freeman about the number of titles requiring license renewal going through the IT department, Mr. Cutright confirmed that DoIT is the central

point of contact, especially for the large applications that are used to run the day-to-day business of the City.

Mr. Lisitano discussed that the Engineering Job Order Contracts (JOC) projects follow-up review was to ensure JOC projects were administered in accordance with established criteria and effective controls were in place. He noted the recommendation was to make sure all supervisors are trained to document all review of projects documents on the summary form. (See Pages 21 and 22 of Attachment 1)

Mr. Lisitano noted the annual credit card security review is a citywide review of operational compliance with Payment Card Industry Data Security Standards (PCI DSS). He stated the standards apply to any organization that accepts, transmits, or stores cardholder data and requires annual assessments. (See Page 24 of Attachment 1)

Mr. Lisitano remarked the follow-up review deals with the operational side for departments that handle credit card transactions in-person and ensures all employees handling credit cards are trained, policies and procedures are maintained and enforced, and risks are mitigated. (See Page 25 of Attachment 1)

Mr. Lisitano reviewed the previous year's recommendations that have been successfully implemented. (See Page 26 of Attachment 1)

Mr. Lisitano pointed out the credit card review this year exhibited issues in Library Services surrounding credit card training not being completed timely and employees sharing logins and passwords within Parks, Recreation, and Community Facilities. He discussed the recommended changes to correct the issues. (See Page 27 of Attachment 1)

Mr. Lisitano advised that management agreed with the recommendations and are implementing the changes. He continued by saying staff will work with the departments to establish the changes and will follow up next year. (See Page 28 of Attachment 1)

In response to a question from Committeemember Luna, Mr. Lisitano clarified the credit card review is not employees using their P-cards but is customer credit card transitions.

3. Adjournment.

Without objection, the Audit, Finance & Enterprise Committee meeting adjourned at 5:02 p.m.

I hereby certify that the foregoing minutes are a true and correct copy of the minutes of the Audit, Finance & Enterprise Committee meeting of the City of Mesa, Arizona, held on the 8th day of December 2021. I further certify that the meeting was duly called and held and that a quorum was present.


DEE ANN MICKELSEN, CITY CLERK

City Auditor

Presentation to the Audit, Finance, and Enterprise Committee
December 8, 2021
Joseph Lisitano, City Auditor

Reports Issued July – Dec 2021



Business Services/Purchasing Division – Procurement Processes



Fleet Services – Parts Management



DoIT – Software/Application Asset Management



Engineering – JOC Projects Follow-up Review



Annual Credit Card Review

Business Services/Purchasing Division – Procurement Processes

Report Date: 11/3/2021

An audit to determine whether effective controls are in place over procurement processes to prevent or detect errors, fraud, waste, or abuse, and ensure compliance with policies, statutes, and other applicable requirements.

Procurement Processes

What did we audit and why?

- Interviewed Purchasing staff and reviewed procedures to identify and determine the effectiveness of internal controls.
- Sampled and tested the following purchases:
 - Small (\$5,000 - \$25,000)
 - Large (> \$25,000)
 - Sole Source
 - Competition Impractical
 - Emergency Purchases
 - Cooperative Contracts
- Analyzed Purchasing's annual commodity spend review.
- Why? To verify effective controls are in place over procurement processes.

Purchasing Processes

What did we find/ recommend?

Conflict of interest is not always specifically addressed as part of the documented procurement activities.

Recommendations:

- Update existing forms to include conflict of interest documentation.
- Retain form/document with other procurement related files.

Purchasing Processes

Cooperative contract agreements were not always properly approved, and lead agencies were not recently verified to be in line with City competitive selection requirements.

What did
we find/
recommend?

Recommendations:

- Develop a process to ensure a written agreement is in place prior to using cooperative contracts.
- Confirm that cooperative agencies use methods in alignment with City competitive selection requirements at initial use and every five years after.

Purchasing Processes

Response & Follow-up

- Management agrees with the recommendations and is implementing corrective action plans.
- All changes should be completed by 1/31/2022.
- We will remain engaged with the department throughout the process to help ensure successful implementation.
- We will perform a follow-up review in approximately 1 year.

Fleet Services – Parts Management

Report Date: 11/8/2021

An audit to determine whether effective controls are in place over parts management to prevent or detect errors, fraud, waste, or abuse and ensure compliance with policies and other applicable requirements.

Parts Management

What did we audit and why?

- Interviewed and observed Fleet Services staff and reviewed policies and procedures to gain an understanding of program operations.
- Sampled and tested the following:
 - Adjustments to inventory
 - Issued parts
 - Inventory count
- Reviewed and analyzed access to both parts system and warehouse facilities.
- Reviewed performance measure goals.
- Why? To verify effective controls are in place over parts management.

Parts Management

What did we find/ recommend?

Parts Management did not always follow their written policies and procedures to ensure an accurate inventory.

Recommendations:

- Enforce written polices by performing:
 - Perpetual inventory counts
 - Count verifications
 - Spot checks
 - Consignment counts
- Modify existing policies and procedures to reflect a more appropriate and reasonable frequency in performing counts.

Parts Management

What did we find/ recommend?

Physical access to the parts warehouse is not restricted.

Recommendations:

- Restrict physical access, including limited distribution of keys, to the parts warehouse to only parts specialists and other personnel deemed necessary.
- Develop and implement policies and procedures to address physical security measures such as:
 - Granting and revoking badge and key access.
 - Periodically review employee access rights.
 - Periodically review security footage and badge access reports to monitor for unauthorized activity.

Parts Management

What did we find/ recommend?

No written policies and procedures in place for disposing of inactive and obsolete parts.

Recommendation:

- Develop and implement written policies and procedures to comply with MCP 100 and 205.

The benchmark criteria used to measure Parts Management performance is not supported with documentation.

Recommendation:

- Maintain documentation to support benchmark criteria.

Parts Management

Response & Follow-up

-
- Management agrees with the recommendations and is implementing corrective action plans.
 - All changes should be completed by 10/31/2022.
 - We will remain engaged with the department throughout the process to help ensure successful implementation.
 - We will perform a follow-up review in approximately 1 year.

DoIT – Software/Application Asset Management

Report Date: 12/1/2021

An audit to determine whether effective controls are in place to ensure all applications used to conduct City business are licensed, inventoried, and meet City IT security standards.

Software/Application Asset Management

Background

- Applications and software from many different providers across all City departments are used to conduct operations.
- DoIT is responsible for managing and maintaining City applications and protecting City against attacks.
- DoIT estimates approximately 1,400 unique titles and 279 titles that require license renewals.
- New asset management system implemented in April 2019.
 - Software assets still being transferred.
 - Once transferred, DoIT can better manage inventory and licenses.

Software/Application Asset Management

What did we audit and why?

- Interviewed DoIT staff to gain an understanding of department procedures and inventory management system.
- Reviewed department policies and procedures.
- Sampled applications and tested for inventory management, licensing, and tech checks.
- Why? To verify effective controls are in place to ensure all applications used to conduct City business are licensed, inventoried, and meet City IT security standards.

Software/Application Asset Management

What did we find/ recommend?

The asset management system used for the inventory of software/applications is not complete or accurate.

Recommendations:

- Complete transition from prior system to new system.
- Conduct a Citywide inventory of software/applications.
- Perform periodic reconciliations between the asset management system and end user systems.
- Consider requiring departments to complete an annual inventory and report the results to DoIT.

Software/Application Asset Management

What did we find/ recommend?

Recommendations (cont.):

- Update policies and procedures to clearly state that software/application purchases must be approved by DoIT.
- Review purchasing reports to ensure software/application purchases are recorded in the asset management system.
- Periodically review the asset management system for completeness and accuracy.
- Consider an effective use of the chart of accounts to ensure software/application purchases are approved and accurately recorded.

Software/Application Asset Management

**What did
we find/
recommend?**

Licenses for software/applications are not effectively tracked or monitored.

Recommendation:

- Implement a formal method to track and monitor software/application license compliance.

Software/Application Asset Management

Response & Follow-up

-
- Management agrees with the recommendations and is implementing corrective action plans.
 - All changes should be completed by 12/1/2022.
 - We will remain engaged with the department throughout the process to help ensure successful implementation.
 - We will perform a follow-up review in approximately 1 year.

Engineering – JOCC Projects Follow-up Review

Report Date: 11/20/2021

A follow-up review to ensure action plans were successfully implemented.

POC Projects Follow-up Review

**What did
we find?**

Status of recommendations from April 2021
report:

- ✓ Engineering should ensure all supervisors are trained to document their review of project documents on the Project Summary form.

✓ Implemented

Annual Credit Card Security Review

Report Date: 7/22/2021

A citywide review of operational compliance with Payment Card Industry Data Security Standards (PCI DSS).

Annual Credit Card Security Review

What is PCI DSS?

- Payment Card Industry Data Security Standard.
- A comprehensive system of operational and technological controls designed to protect cardholder data.
- Applies to any organization that accepts, transmits, or stores any cardholder data.
- Annual assessments are required.
- Compliance is a constant challenge due to staff turnover and evolving requirements.

Why do we audit this every year?

Annual Credit Card Security Review

What did we audit?

Compliance with operational requirements:

- Screening and training all employees and volunteers who handle credit cards.
- Maintaining and enforcing PCI DSS compliant policies and procedures at all acceptance sites.
- Mitigating risks related to contracted third-party payment processing service providers.
- Remediating non-compliance when found.

Annual Credit Card Security Review

Last year's recommendations were successfully implemented:

- ✓ Maintain up-to-date list of POS device and document inspections. (PRCF)
- ✓ Conduct and document inspections of POS devices to meet PCI DSS and City requirements. (PRCF)
- ✓ Implement a control to ensure new credit card handlers complete training within 3 months. (Arts & Culture)
- ✓ Implement a control to ensure that all credit card handlers complete training within required time frames. (PRCF)

Follow-up:

What did we find?

✓ Implemented

Annual Credit Card Security Review

**This year:
What did
we find/
recommend?**

This year's review found:

- 1. Credit card training not being completed within required time frames. (Library Services)**
 - Recommended implementation of a control to ensure training is completed within required timeframes.
- 2. Employees are sharing logins and passwords. (PRCF)**
 - Recommended that a unique login and password is assigned to each user accessing any system used to process credit card transactions.

Annual Credit Card Security Review

Response & Planned Follow-up

- Management from each of the departments involved agreed with the recommendations and will implement the changes.
- We will communicate with the departments throughout the year to help ensure successful implementation and continued compliance.
- We will follow-up at the next annual review.

Questions?

m.e.s.a.az

