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

What did we find/ recommend?

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

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 – JOC Projects Follow-up Review

Report Date: 11/20/2021

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

JOC 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?

Why do we audit this every year?

- 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.

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

Follow-up: What did we find?

✓ Implemented

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)

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?