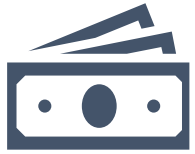
City Auditor

Presentation to the Audit, Finance and Enterprise Committee
June 26, 2025
Joseph Lisitano, City Auditor

Reports Issued May – June 2025



Citywide Cash Handling

DoIT – Software/Application Management Follow-up Review

DoIT – Cybersecurity

Citywide Cash Handling

Report Date: 6/30/2025

Biennial report on citywide audits of cash handling, change funds, and petty cash.

Citywide Cash Handling

What did we audit and why?

Throughout the period, we verify:

- Compliance with City policies and procedures.
- Petty cash and change fund balances.

Goals:

- Early detection to avoid significant issues.
- Deterrence and consistent enforcement of compliance.
- Relationships – answer questions/concerns; offer help when possible.

Citywide Cash Handling

What did we find?

- No material discrepancies in fund balances.
- Issues related to cash handling training.
- Overall, effective processes in place to safeguard cash.

Citywide Cash Handling

What did we recommend?

Library Services should implement improved internal controls to ensure all employees receive training within the required timeframes.

Citywide Cash Handling

Response & Follow-up

- Management agrees with the recommendation and has begun implementing new controls.
- We will perform follow-up work as part of the FY2027 Citywide cash handling audit.

DoIT – Software/Application Asset Management Follow-up Review

Report Date: 5/15/2025

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

DoIT – Software Application Asset Management Follow-up Review

What did we find?

Status of recommendations from December 2021 report:

- ✓ Complete the transition of assets from the prior asset management system to the new management 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 software/application inventory and report the results to DoIT.

✓ Implemented

♦ In Progress

DoIT – Software Application Asset Management Follow-up Review

What did we find?

Status of recommendations from December 2021 report:

- Update policies and procedures to clearly state that software/application purchases must be approved by DoIT.
- Review purchasing reports to ensure software/application purchases (especially p-card 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 Account codes to ensure software/application purchases are approved by DoIT and accurately recorded in the asset management system.
- A formal method to track and monitor software/application license compliance should be implemented.

✓ Implemented

♦ In Progress

DoIT – Software Application Asset Management Follow-up Review

Follow-up

- We will perform a second follow-up review in approximately 9 months.
- We will remain engaged with the department throughout the process to help ensure successful implementation.

DoIT – Cybersecurity

Report Date: 6/19/2025

An audit to determine whether effective controls are in place that would help prevent, deter, and/or respond to cyberattacks.

DoIT – Cybersecurity

What did we audit and why?

- Evaluated against the CIS Critical Security Controls, Implementation Group 2.
- Interviewed and performed walk-throughs with DoIT staff to gain an understanding of controls in place.
- Reviewed policies and procedures, DoIT standards, incident response and disaster recovery/business continuity plans, and inventory listings.
- Tested a sample of user accounts, including administrator and service accounts, and terminated employees.
- Reviewed documentation of vulnerability scans, audit logs, penetration test results, incident response exercises, and automated data backups and recovery tests.

DoIT – Cybersecurity

What did we audit and why?

- Examined third-party service provider contracts.
- Reviewed security awareness training materials and training certificates.
- Verified tools have been implemented to aggregate threat intelligence, manage software vulnerabilities and automated patch updates, and identify and monitor assets.
- Verified the use of firewalls, virtual private network (VPN), multi-factor authentication (MFA), anti-malware software, and networking monitoring tools.
- Reviewed network infrastructure diagrams, baseline configuration templates, and network traffic flow logs.
- Why? To ensure effective controls are in place that would help prevent, deter, and/or respond to cyberattacks.

DoIT – Cybersecurity

What did we find and recommend?

Several safeguards described in the CIS Controls have not yet been developed and implemented or could be further improved.

Recommendation:

- Due to the sensitive nature of the findings contained in the report, we recommend an executive session to discuss the issues and recommendations.

Questions?