City Auditor

Presentation to the Audit, Finance and Enterprise Committee
April 7, 2025
Joseph Lisitano, City Auditor

Reports Issued July 2024 – March 2025

- Police – Criminal Investigations Case Management
- Department of Innovation and Technology – Remote Access
- Citywide – Intergovernmental Agreements Cost Recovery
- Community Facilities Districts
- Citywide – Annual Credit Card Security Review
- Police – Badging/Security Access Follow-up Review

Police – Criminal Investigations Case Management

Report Date: 7/15/2024

An audit to determine whether effective controls are in place to ensure that cases are properly assigned, investigated, and disposed of in accordance with applicable policies, statutes, and other requirements.

Police – Criminal Investigations Case Management

What did we audit and why?

- Interviewed Criminal Investigations Division management and staff.
- Reviewed Police Department policies to gain an understanding of department operations for case management.
- Selected a sample of 60 homicide, sex crimes, and child abuse cases; and reviewed case report narratives to determine if the cases were investigated timely and appropriately.
- Why? To verify effective controls are in place to ensure criminal cases are investigated and disposed of in accordance with applicable requirements.

Police – Criminal Investigations Case Management

What did we find and recommend?

Timely and/or appropriate case follow-up could not always be determined

Recommendation:

- To ensure timely and appropriate investigation of cases, management should:
  - Review open cases at least monthly and follow-up with detectives, as necessary.
  - Require dates to be added to report narratives.
  - Require additional documentation in report narratives if there are delays in the investigation.
  - Implement a process to ensure timely reassignment of cases when a detective retires or leaves the department.
  - Determine if additional supervisor review or documentation is necessary if an attorney has been requested for a case.

Police – Criminal Investigations Case Management

Response and Follow-up

- Management agrees with the recommendation and is implementing a corrective action plan.
- 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 – Remote Access

Report Date: 7/16/2024

An audit to determine whether effective controls are in place to ensure risks related to remote access to the City's network are minimized and connectivity between the network and remote users is secure.

DoIT – Remote Access

What did we audit and why?

- Interviewed DoIT personnel.
- Reviewed policies and procedures and observed processes to gain an understanding of remote user access, including the process for managing remote access VPN.
- Reviewed employment contracts and background check certification forms for third-party workers.
- Selected a sample of active employees, terminated employees, and third-party workers to ensure remote user access was properly granted, revoked, and monitored.
- Why? To verify effective controls are in place to ensure risks to the City's network are minimized when accessing it remotely.

DoIT – Remote Access

What did we find and recommend?

The department does not have formal polices and procedures for managing remote access VPN

Recommendation:

- The department should develop and implement policies and procedures for managing remote access VPN that address the following:
  - Roles and responsibilities of staff involved in VPN management.
  - The process for ensuring its VPN client is secure and undergoes the required scheduled maintenance.
  - The process for detecting and responding to VPN-related issues, including establishing an incident response plan for addressing incidents such as VPN security breaches.
  - Continuously reviewing and updating its policies and procedures to ensure it appropriately addresses evolving security threats and advances in VPN technology.

DoIT – Remote Access

Response and Follow-up

- Management agrees with the recommendation and is implementing a corrective action plan.
- 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.

Citywide – Intergovernmental Agreements Cost Recovery

Report Date: 3/27/2025

An audit to determine whether effective controls are in place for select City of Mesa intergovernmental agreements to ensure costs are recovered in accordance with the applicable agreement and any other applicable policies, statutes, and other requirements.

Citywide – Intergovernmental Agreements Cost Recovery

What did we audit and why?

- Interviewed City department staff.
- Reviewed policies and procedures and other documentation to gain an understanding of City department processes related to IGAs with cost recovery components.
- Performed a walk-through of the IGA database maintained by the Real Estate Services Division.
- Tested a sample of IGAs, invoices, and revenue reports to determine if costs were properly recovered based on the terms and conditions of the agreement.
- Why? To verify effective controls are in place to ensure the City is appropriately recovering costs as part of their IGAs.

Citywide – Intergovernmental Agreements Cost Recovery

What did we find and recommend?

City departments do not have a process in place to ensure they are complying with Management Policy 119

Recommendation:

- To comply with Management Policy 119, management should develop and implement a process to ensure all signed and executed IGAs are electronically stored and filed with Real Estate Services within the Engineering Department.

Citywide – Intergovernmental Agreements Cost Recovery

What did we find and recommend?

City departments do not have written policies and procedures in place to ensure costs are fully recovered

Recommendation:

- To help ensure costs are fully recovered, departments should develop and implement policies and procedures to address the following:
  - The process for preparing invoices to ensure the proper amount, including ensuring only reimbursable costs, was invoiced.
  - The process for tracking payments to ensure all costs have been fully recovered.

Citywide – Intergovernmental Agreements Cost Recovery

Response and Follow-up

- Management agrees with the recommendations and is implementing a corrective action plan.
- We will remain engaged with the departments throughout the process to help ensure successful implementation.
- We will perform a follow-up review in approximately 1 year.

Engineering – Community Facilities Districts

Report Date: 3/24/2025

An audit to determine whether issued bonds for the City's Community Facilities Districts were used to only reimburse projects in compliance with applicable policies, statutes, and other requirements.

Engineering – Community Facilities Districts

What did we audit and why?

- Interviewed City department staff.
- Reviewed Arizona Revised Statutes to gain an understanding of the statutes and other requirements applicable to CFD projects.
- Tested a sample of CFD projects by reviewing project documentation, City Council resolutions, developer project reimbursement requests, and CFD Bond Official Statements.
- Why? To ensure issued bonds were only used to reimburse CFD projects in compliance with applicable policies, statutes, and other requirements.

Engineering – Community Facilities Districts

What did we find and recommend?

In our opinion, effective controls are in place to ensure that issued bonds are only being used to reimburse projects that are in compliance with applicable policies, statutes, and other requirements.

Citywide – Annual Credit Card Security Review

Report Date: 3/27/2025

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

Citywide – 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.

Why do we review this every year?

- 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.

Citywide – Annual Credit Card Security Review

What did we review?

Compliance with operational requirements:

- Screening and training all employees and volunteers who handle cardholder data.
- 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.

Citywide – Annual Credit Card Security Review

This year: What did we find and recommend?

This year's review found:

Credit card handling training not being completed within required timeframes (Business Services, Library Services, and Development Services)

- Recommended implementation of a control to ensure training is completed within required timeframes.

Citywide – Annual Credit Card Security Review

Response and Follow-up

- Management from each department agreed with the recommendation and will implement the corrective action plan.
- 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.

Badging/Security Access – Follow-up Review

Report Date: 12/23/2024

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

Badging/Security Access – Follow-up Review

What did we find?

Status of recommendations from November 2022 report:

- ✓ Ensure forms are properly completed before issuing ID badges or granting access to City facilities by implementing one or more of the following:
  - ✓ Updating forms to make it clear supervisor approval must be obtained before badges will be issued/access granted.
  - ✓ If other verification methods are used in place of obtaining supervisor approval, the verification should be documented in the individual's file.
  - ✓ Creating internal Badging Office policies and procedures that document the other verification methods that can be used in lieu of supervisor approval.
- ✓ Management should establish a process to ensure all badges are returned after termination or evaluate the risk of badges not being returned and update the Management Policy as appropriate.

✓ Implemented

Questions?