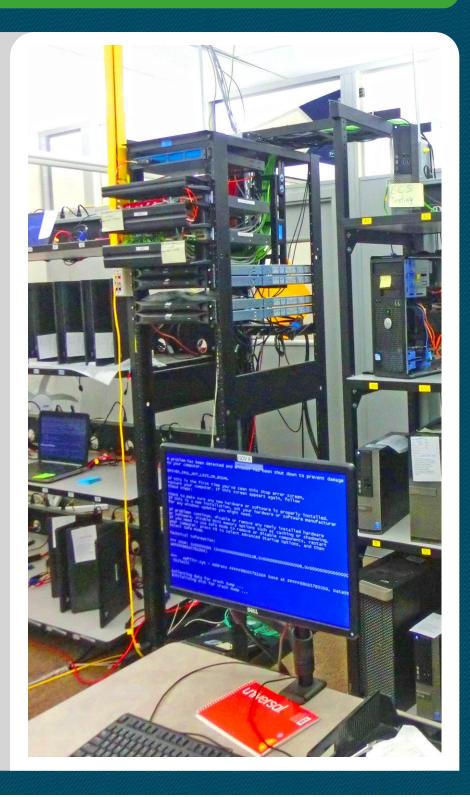# FOLLOW-UP REPORT
Information Technology
Asset Management Audit
February 2018

Office of the Auditor
Audit Services Division
City and County of Denver

Timothy M. O'Brien, CPA
Denver Auditor

The Auditor of the City and County of Denver is independently elected by the citizens of Denver. He is responsible for examining and evaluating the operations of City agencies and contractors for the purpose of ensuring the proper and efficient use of City resources and providing other audit services and information to City Council, the Mayor, and the public to improve all aspects of Denver's government.

The Audit Committee is chaired by the Auditor and consists of seven members. The Audit Committee assists the Auditor in his oversight responsibilities regarding the integrity of the City's finances and operations, including the reliability of the City's financial statements. The Audit Committee is structured in a manner that ensures the independent oversight of City operations, thereby enhancing citizen confidence and avoiding any appearance of a conflict of interest.

Audit Committee

Timothy M. O'Brien, CPA, Chairman

Rodolfo Payan, Vice Chairman

Jack Blumenthal

Leslie Mitchell

Florine Nath

Charles Scheibe

Ed Scholz

Audit Management

Timothy M. O'Brien, CPA, Auditor

Valerie Walling, CPA, CMC®, Deputy Auditor

Heidi O'Neil, CPA, CGMA, Director of Financial Audits

Kevin Sear, CPA, CIA, CISA, CFE, CGMA

Audit Team

Shannon Kuhn, CISA, IT Audit Supervisor

Brian Cheli, CISA, CISSP, Senior IT Auditor

Joah Flood, MBA, Staff Auditor

You can obtain copies of this report by contacting us:

Office of the Auditor

201 West Colfax Avenue, #705

Denver CO, 80202

(720) 913-5000 ⬥ Fax (720) 913-5247

Or download and view an electronic copy by visiting our website at: www.denvergov.org/auditor

Audit report year: **2016**

City and County of Denver

201 West Colfax Avenue, #705 ● Denver, Colorado 80202

720-913-5000 ● Fax 720-913-5253 ● www.denvergov.org/auditor

Timothy M. O'Brien, CPA
Auditor

February 1, 2018

Mr. Stephen Coury, Chief Information Security Officer, Technology Services
Ms. Kelli Bennett, Financial Director, Controller's Office
Ms. Jessica Chandler, Financial Manager, Controller's Office
City and County of Denver

Re: Audit Follow-Up Report

Dear Mr. Coury, Ms. Bennett, and Ms. Chandler:

In keeping with generally accepted government auditing standards and the Audit Services Division's policy, as authorized by D.R.M.C. § 20-276, our division has a responsibility to monitor and follow up on audit recommendations to ensure findings are being addressed through appropriate corrective action and to aid us in planning future reports.

This letter is to inform you we have completed our follow-up effort for the Information Technology Asset Management audit issued April 21, 2016. The audit made seven recommendations, four to Technology Services and three to the Controller's Office. Our follow-up review determined that Technology Services fully implemented three recommendations but has yet to fully implement the fourth. Of the three recommendations directed to the Controller's Office, one was fully implemented, one was partially implemented, and one was not implemented. As a result, our office may revisit these risk areas in future audits to ensure appropriate corrective action is taken.

For your reference, this report includes a highlights page that provides background and summary information on the original audit and the completed follow-up effort. Following the highlights page is a detailed implementation status update for each recommendation.

This concludes audit follow-up work related to this audit. I would like to express our sincere appreciation to you and to Technology Services and Controller's Office personnel who assisted us throughout the audit and follow-up process. If you have any questions, please feel free to contact me at 720-913-5000 or Shannon Kuhn, Internal Audit Supervisor, at 720-913-5159.

Denver Auditor's Office

Timothy M. O'Brien, CPA
Auditor

Information Technology Asset Management Audit

February 2018

Status

Technology Services implemented three recommendations but only partially implemented a fourth. The Controller's Office implemented one recommendation, partially implemented a second, and did not implement a third.

Background

Information Technology asset management is a process used to catalog and record IT equipment, desktop and laptop computers, and servers. The process is designed to monitor IT assets throughout the life cycle of the equipment from the initial purchase through disposal. Agency custodians, Technology Services (TS), and the Controller's Office have responsibility for keeping the City's IT asset financial system of record current.

Purpose

The objective of the audit was to assess the IT asset management process over desktop computers, laptop computers, and servers, including assessing whether the City's financial system of record is complete and accurate and whether assets are properly tracked and safeguarded.

REPORT HIGHLIGHTS

Highlights from Original Audit

The audit identified that the City needed to take further action to improve the Information Technology (IT) asset management process. The following areas of concern related to the completeness and accuracy of the inventory system of record, the physical security of the City's computer assets, and communication, training, and policies related to the process:

- The final disposition for all audited IT assets could not be accounted for, which resulted in inaccuracy in the system of record.

- Computer data storage media, such as hard drives and backup tapes, designated for disposal were stored in an unsecure location that was publicly accessible within the TS department.

- Agency asset custodians had not been provided with adequate communication and training regarding the new IT asset inventory process.

- Technology Services' policy did not reflect the new IT asset management process and it had not been updated for a few years. Additionally, while the policy documented the process for transferring unused IT assets, it did not provide clear, precise timeframes on when this was expected to be performed.

- Technology Services' policy did not provide guidance for agencies if IT equipment were lost or stolen.

- Inaccurate asset profile IDs existed in the City's financial system of record.

Identified IT asset management weaknesses increased risks of ineffective utilization of these assets, as well as a posed a greater risk for fraud and abuse. We offered several recommendations to mitigate these risks.

Findings at Follow-up

Although Controller's Office personnel provided communication and training to asset custodians in 2016 on how to inventory IT assets, they did not properly train or evaluate asset custodians in 2017, some of whom were new to the role. Further, the Controller's Office has still not established a base inventory for computer assets. Technology Services has secured the inventory of IT equipment slated for disposal and now has appropriate inventory controls over physical assets. Additionally, Technology Services updated policies and communicated the changes to the appropriate parties, ensuring proper governance over IT asset management. Finally, Technology Services established a procedure for recording lost or stolen IT equipment; however, the agency has not yet created a control to update the system of record.

For a copy of this report, visit www.denvergov.org/auditor or contact the Auditor's Office at 720-913-5000.

Recommendations: Status of Implementation

Recommendation	Auditee Action	Status
FINDING: Weaknesses Exist with the City's Process for Managing Information Technology Assets		
1.1 The Controller's Office should work with the Chief Information Officer in Technology Services to ensure that a base inventory is established for all audited IT assets in 2016 and maintain the inventory through periodic reviews of changes in asset inventory such as purchase of new equipment and disposed assets.	Although requested on multiple occasions, the Controller's Office has not provided auditors with a complete listing of a base inventory. We received a list of IT assets with a corresponding profile number, as well as a list of disposed and unknown assets. However, these documents do not constitute a complete base inventory from the Controller's Office.	**Not Implemented** **Original target date for completion: September 30, 2016**
1.2 The Controller's Office should work with the Chief Information Officer in Technology Services to provide an annual mandatory training and communication to the agency asset custodians on the inventory and asset management processes for IT assets. In addition, the Controller's Office and Technology Services should ensure the right person is in the agency asset custodian role annually and request the agency to assign a new custodian if needed.	The Controller's Office provided communication and inventory training to agency asset custodians in July 2016. However, the office did not provide training to agency asset custodians in 2017 because there were no changes to the process, even though there were several agency custodians who had been assigned to the role since the 2016 training. In September 2017, the Controller's Office communicated to agency authorities the importance of each agency's responsibilities regarding asset management and asked to verify that their asset custodian(s) were the appropriate people assigned to this role.	**Partially Implemented** **Original target date for completion: June 30, 2016**

Recommendations: Status of Implementation

	Recommendation	Auditee Action	Status
1.3	The Chief Information Officer in Technology Services should ensure that IT equipment designated for disposal, which may contain sensitive or City data, is stored in a secure location that is not publicly accessible. Additionally, we recommend that the Director of Asset Management should notify Technology Services staff through a new policy about the establishment of the secure location.	Technology Services has moved all equipment designated for disposal that may contain sensitive or City data to a secure location not accessible to the public. Technology Services has developed and communicated a policy for IT asset management, which includes the establishment of a secure storage location.	**Implemented**
1.4	The Chief Information Officer in Technology Services should update the Technology Asset Purchasing and Replacement Policy to ensure that it aligns with the new IT asset management process, which includes defining roles and responsibilities regarding IT asset management.	Technology Services updated the existing IT asset management policy and ensured that the new IT asset management process aligns with the policy. In addition, Technology Services has defined roles and responsibilities regarding IT asset management in the appropriate process documentation.	**Implemented**
1.5	The Chief Information Officer in Technology Services should update the Technology Asset Purchasing and Replacement Policy to specify a timeframe by which agencies must transfer unused equipment back to Technology Services for redeployment.	Technology Services updated the existing IT asset management policy, which specifies that unused equipment must be returned within 10 business days.	**Implemented**

Recommendations: Status of Implementation

	Recommendation	Auditee Action	Status
1.6	The Chief Information Officer in Technology Services should establish a procedure for lost or stolen IT equipment that includes a control to update the system of record.	Technology Services established a process for recording lost or stolen IT assets, and has created formal written procedures. However, the agency has not yet finished a process for updating the system of record but expects to do so by January 2018. Between the initial audit and the follow-up report, a decision was made by Technology Services to change the system of record from what the Controller's Office uses to what is most practical for Technology Services, ServiceNow.	**Partially Implemented** **Original target date for completion: October 31, 2016**
1.7	The Controller's Office should perform a clean-up of historical IT asset data prior to the implementation of a new Enterprise Resource Planning solution.	Initial cleanup of historical assets began with email communication between the Controller's Office and Technology Services. In addition, the Controller's Office provided auditors with evidence that a clean up the data has taken place, which eventually led to assurance by the auditor over multiple iterations	**Implemented**

Conclusion

While Technology Services has implemented three recommendations made in our 2016 Information Technology Asset Management audit report, the agency has only partially implemented the fourth. Regarding the final recommendation—regarding establishing a procedure for recording lost or stolen IT equipment—we would note that Technology Services plans to use a system to track and manage lost or stolen IT equipment that does not interface with the system used in the Controller's Office to track and manage all IT equipment. We have concerns that, even though agency asset custodians will manage and track IT equipment using the new process, they will not have the necessary access to update both systems. Training was not provided on the new system of record – Workday – as the Controller's Office stated that inventorying was done in PeopleSoft through 2017's annual asset inventory process. We have received no additional evidence over any training procedures provided to agency asset custodians inventorying assets in Workday.

The Controller's Office has yet to fully implement the three recommendations for which it was responsible. The office did not provide auditors with a base inventory of IT assets citywide and did not provide training to asset agency custodians in 2017. Furthermore, the Controller's Office did not confirm with the agency expending authorities that the asset custodians in place were the right individuals for the custodian position. Without a base inventory of all IT assets, the City remains at risk for lost or stolen equipment that goes unrecorded. Without proper training, assets from each department may not be appropriately reconciled to one of the systems of record.

Despite the efforts of the Controller's Office and Technology Services, auditors determined that the risks identified in our 2016 report have not been fully mitigated. As a result, we may revisit these risk areas in the future to ensure appropriate corrective action is taken.

On behalf of the citizens of the City and County of Denver, we thank staff and leadership from the Controller's Office and Technology Services for their cooperation during our follow-up effort and their dedicated public service.