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 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. He also chairs the City’s Audit Committee.

The Audit Committee is chaired by the Auditor and consists of seven members. The Audit Committee assists the Auditor in his oversight responsibilities of the integrity of the City’s finances and operations, including the integrity 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
Rudolfo Payan, Vice Chairman
Jack Blumenthal
Leslie Mitchell
Florine Nath
Charles Scheibe
Ed Scholz

Audit Management

Valerie Walling, CPA, CMC®, Deputy Auditor
Kip Memmott, MA, CGAP, CRMA, Director of Audit Services

Audit Staff

Shannon Kuhn, CISA, IT Audit Supervisor
Nicholas Jimroglou, CISA, Lead IT Auditor
Karin Doughty, CISA, Senior IT Auditor
Tyler Kahn, Senior IT Auditor

You can obtain copies of this report by contacting us:

Office of the Auditor
201 West Colfax Avenue, Department 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
Report number: A2015-014
AUDITOR’S REPORT

We have completed an audit of Information Technology (IT) Asset Management. The purpose of the audit was to review the current IT asset management process for desktop computers, laptop computers, and servers, and to assess the controls in place to track, inventory, store, retrieve, transfer, and disposed of IT equipment in use throughout the City.

As described in the attached report, our audit revealed that Technology Services (TS) and the Controller’s Office need to fine tune relevant policies and procedures to further safeguard IT assets and ensure success of the City’s IT asset management approach.

Through stronger internal controls, policies, and more frequent communication, TS and the Controller’s Office will be able to improve the overall IT asset management process, and we make several recommendations to this end.

This performance audit is authorized pursuant to the City and County of Denver Charter, Article V, Part 2, Section 1, General Powers and Duties of Auditor, and was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We extend appreciation to TS and the Controller’s Office and the personnel who assisted and cooperated with us during the audit.

Denver Auditor’s Office

Timothy M. O’Brien, CPA
Auditor
Information Technology Asset Management
April 2016

Scope
The audit reviewed the current Information Technology (IT) asset management process to assess the controls in place over tracking inventory as well as storing, retrieving, transferring, and disposing of computer equipment. The audit also evaluated the efficacy of agency asset custodian training.

Background
IT asset management is a process by which to catalogue and record IT equipment, desktop and laptop computers, and servers. The process is designed to monitor IT assets throughout the equipment life cycle from initial purchase through disposal. Agency Custodians, Technology Services (TS) and the Controller’s Office have responsibility for tracking IT assets in the City’s financial system of record.

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.

Highlights
The audit identified that the City needs to take further action to improve the IT asset management process. The following areas of concern relate 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 cannot be accounted for, which results 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 is publicly accessible within the TS department.
- Agency asset custodians have not been provided with adequate communication and training regarding the new IT asset inventory process.
- TS’s policy does not reflect the new IT asset management process and has not been updated for a few years. Additionally, while the policy documents the process for transferring unused IT assets, it does not provide clear, precise timeframes on when this is expected to be performed.
- TS’s policy does not provide guidance for agencies in the event that IT equipment is lost or stolen.
- Inaccurate asset profile ID’s exist in the City’s financial system of record.

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

For a complete copy of this report, visit www.denvergov.org/auditor
Or contact the Auditor’s Office at 720.913.5000
# TABLE OF CONTENTS

**INTRODUCTION & BACKGROUND**  
- Asset Management 1  
- IT Asset Management in the City and County of Denver 1

**SCOPE**  
4

**OBJECTIVE**  
4

**METHODOLOGY**  
4

**FINDING**  
6  
- Weaknesses Exist with the City’s Process for Managing Information Technology Assets 6  
- Opportunities Exist To Improve the Inventory Process for Information Technology Assets 6  
- Technology Services’ Existing Policy Needs to Be Updated 10

**RECOMMENDATIONS**  
14

**APPENDIX**  
16  
- Grant Thornton Audit 16

**AGENCY RESPONSE**  
32
INTRODUCTION & BACKGROUND

Asset Management

Asset Management is the process of recording and tracking something of value from the purchase, receipt, and ongoing maintenance throughout the life of the asset.\(^1\) Gartner, a leading Information Technology (IT) research and advisory firm, describes Information Technology Asset Management (ITAM) in the following way:

\[
\text{ITAM entails collecting inventory, financial and contractual data to manage the IT asset throughout its life cycle. ITAM depends on robust processes, with tools to automate manual processes. Capturing and integrating auto-discovery/inventory, financial and contractual data in a central repository for all IT assets enables the functions to effectively manage vendors and a software and hardware asset portfolio from requisition through retirement, thus monitoring the asset’s performance throughout its life cycle.}^{\!2}\]

IT assets are critical to the productivity of employees in today’s workplace, meaning it is important that management properly tracks and deploys IT equipment to staff. An effective IT asset management process is key to ensuring that an organization is consistently able to provide employees with the IT tools needed to perform their jobs.

In accordance with the City’s Fiscal Accountability Rule 4.2, there are two categories of IT assets: controlled and capitalized. Controlled assets have an acquisition cost ranging from $500 to $4,999.99. Controlled IT assets include servers, scanners, printers, desktop computers, laptop computers, and tablets. Capitalized assets have a purchase price of $5,000 and greater. Capitalized IT assets include high-end servers and certain enhanced-capability desktop and laptop computers.

IT Asset Management in the City and County of Denver

The following personnel and City agencies have core IT asset management responsibilities: Asset custodians in agencies, Technology Services, Controller’s Office and the Agencies.

Agency Asset Custodians—Agency asset custodians are responsible for managing and maintaining the IT assets within their agencies.

Technology Services—Technology Services (TS) is the City agency responsible for managing computers and applications, products, and services. Desktop support personnel support the operations of IT assets by configuring new equipment, replacing old equipment, and troubleshooting computer issues. In 2015, TS’s budget for operating expenses was approximately $21 million, budgeted for services and supplies, including desktop computers, laptop computers,

---

\(^1\) In accordance with the City’s Fiscal Accountability Rule 4.2, the term asset refers to anything tangible or intangible that is capable of being owned or controlled to produce value. This includes things like cash, accounts receivable, and inventory. Fixed assets are those that are expected to keep providing benefit for more than one year, such as equipment, buildings, and real estate.

and servers. The City has a master purchase agreement with Dell Marketing to supply the City with desktop and laptop computers, with an average price of $600 and $1,000, respectively.

TS manages over 9,000 desktops and laptops distributed throughout a large geographic area for 30 agencies and component agencies. This pool of assets is constantly in motion as employees are hired, change locations, and separate from the City. IT equipment follows an asset lifecycle, which begins with procurement and ends with disposal. The purpose of the lifecycle is to manage an asset through each phase of the asset’s useful life. TS designates the useful life of a computer—both desktop and laptop—to be five years.

Controller’s Office—The Controller’s Office is responsible for financial reporting for the City. This includes maintaining an inventory of all controlled and capitalized IT assets within PeopleSoft, which is the City’s current financial system of record (SOR). The IT asset inventory process is managed by the Director of Accounting and Financial Reporting.

Governance of IT Assets—IT asset management is primarily governed by the following two policies:

- **Technology Asset Purchasing and Replacement Policy**—This policy was established to ensure that there is standardization for IT equipment through the City; that computers are adequately deployed to employees; and that TS is included in all IT equipment purchasing decisions. Additionally, the policy documents the process for transferring unused IT assets.

- **Fiscal Accountability Rule 4.2**—FAR 4.2 is the key policy that defines asset types as well as the roles and responsibilities for managing and safeguarding assets.

**IT Asset Lifecycle**

The lifecycle of an IT asset begins with an agency or TS requesting to purchase new computer equipment. TS then approves the associated purchase order and, in most cases, physically receives the asset. Once the IT asset is received, TS configures it in accordance with the agency’s needs and delivers it to the user. Throughout the useful life of an IT asset, TS maintains the equipment by providing regular software updates, virus patches, and support. An agency as well as TS can dispose of an IT asset that is past its useful life. The City has a contract with METech Recycling, a computer disposal company, which recycles City IT equipment that has exceeded its useful life. Improperly disposing of IT equipment can introduce toxic materials into the environment. METech’s recycling operations are in compliance with U.S. Environmental Protection Agency guidelines and federal and state laws for disposing of IT equipment. Using a third-party recycler also ensures secure removal of sensitive data to prevent data loss. See Figure 1 for a flow chart of the IT asset lifecycle.
Recent Changes to the City’s IT Asset Management Process

In 2015, the City changed the process for inventorying IT assets. Previously, IT assets were tracked in the SOR and agency asset custodians were responsible for conducting physical inventories on an annual basis. In the SOR, the records for these assets indicated that the individual agencies were the assigned custodian. Currently, to help carry out the inventory process, TS utilizes a discovery tool to locate IT assets that are connected to the City’s network. The SOR now reflects TS as the custodian of these assets in the custodian field of the SOR. However, agency asset custodians still retain the responsibility of safeguarding IT assets that are used by employees in their agencies. In addition, agency asset custodians are responsible for updating the SOR should an asset change location or become lost or stolen and performing a yearly physical inventory for all assets assigned to the agency.
SCOPE

The audit reviewed the current Information Technology (IT) asset management process to assess the controls in place over tracking inventory as well as storing, retrieving, transferring, and disposal of computer equipment. The audit also evaluated the efficacy of agency asset custodian training. The audit scope was limited to servers and workstations, including desktop and laptop computers. The City’s financial system of record, PeopleSoft, was assessed to determine its completeness and accuracy.

OBJECTIVE

The objective of the audit was to assess the efficiency and effectiveness of the IT asset management process over desktop computers, laptop computers, and servers as administered by Technology Services (TS), the Controller’s Office, and agency asset custodians. The objective included assessing asset reconciliation processes to determine whether the City’s financial system of record is complete and accurate and whether assets are safeguarded and tracked throughout their lifecycles.

METHODOLOGY

To achieve the audit objective, we used the following audit methodologies:

- Consulting best practice standards, including the Federal Information System Controls Audit Manual (FISCAM) and standards promulgated by the National Institute of Standards and Technology (NIST)
- Conducting interviews and walk-throughs with agency asset custodians, the Controller’s Office, and TS on their understanding of the new and old asset management processes
- Interviewing TS IT Asset Managers and Controller’s Office personnel responsible for updating the PeopleSoft system of record (SOR) with IT asset data
- Observing storage of IT equipment in inventory
- Examining IT asset management policies and procedures
- Conducting a survey to gain an understanding of agency asset custodians’ knowledge of their IT asset management process, including documentation and training provided by the Controller’s Office
- Evaluating a sample of equipment for inclusion in PeopleSoft, timely deployment of new equipment, and validating the reporting of lost or stolen equipment
- Reviewing relevant audits conducted nationwide and in Canada and comparing them to baseline best practice standards
- Reviewing the findings of a prior asset management audit performed by Grant Thomton, an independent audit, tax, and advisory firm
- Understanding the lifecycle of an IT asset from purchase through use, disposal, and replacement as established by TS
• Reviewing a City contract with Dell Marketing for terms and conditions related to IT equipment purchases
• Reviewing a City contract with METech Recycling for terms and conditions related to secure disposal of IT equipment and components
• Observing the location and security of IT equipment scheduled for disposal
• Reviewing agency asset custodians’ annual inventory workbooks and compare to SOR
FINDING

Weaknesses Exist with the City’s Process for Managing Information Technology Assets

Managing the City’s information technology (IT) assets is the collective responsibility of multiple parties, notably the Controller’s Office, Technology Services (TS), and designees within the agencies that use the assets. In assessing how these assets are being managed, we identified two general areas for improvement. First, the inventory process could be improved to achieve a more accurate record of IT assets, additional training needs to be provided for City personnel involved in the process, and the security of assets that are about to be retired needs to be enhanced. Second, a key policy governing the management of IT assets needs to be updated to accurately reflect the current inventory process. Specifically, the policy needs to be clarified to better manage assets that are no longer in use, and expanded to provide guidance regarding how to code these assets in the City’s financial system of record (SOR). By improving these two areas, TS and the Controller’s Office will be able to better ensure the integrity of the City’s financial records and the security of confidential City data.

Opportunities Exist To Improve the Inventory Process for Information Technology Assets

In 2015, TS assumed the role of IT asset custodian in the SOR from the agency asset custodians. The inventory process for controlled and capitalized assets was used to transfer the custodianship of IT assets from the agency asset custodians to TS. In assessing the IT asset inventory process, audit work found several areas in need of improvement. First, the SOR may not accurately reflect all audited IT assets, reducing the likelihood that the City has established a complete inventory of IT assets. Specifically, the final disposition of some IT assets cannot be accounted for, presenting uncertainty regarding the security of any sensitive and confidential data that may have been on the assets. Second, additional training and communications regarding the new inventory process may need to be provided to agency asset custodians to ensure that all IT assets are accounted for in 2016 and that the process is efficiently executed. Lastly, we found that some hard drives awaiting disposal were not properly secured, exposing the City to the potential of losing sensitive and confidential data.

The System of Record May Not Accurately Reflect All Information Technology Assets

PeopleSoft is the SOR that comprises all controlled and capitalized assets for each City agency. In 2015, the custodian role of all controlled IT assets was transferred from the agency asset custodians to TS by utilizing an electronic discovery tool, System Center Configuration Manager (discovery tool), to locate IT assets that were active on the City’s network. However, not all IT assets were connected to the network, creating a variance between the SOR and the assets located by the discovery tool. At the time of the audit, approximately 800 IT assets were still being reviewed to determine their disposition. The uncertainty regarding the assets prevents the City from achieving a complete inventory and demonstrates that there are some areas where
controls can be improved to mitigate losing sensitive and confidential data that may be associated with the assets in review.

To initiate the transition of IT assets from the agency asset custodians to TS and to compile the 2015 inventory of IT assets, the Controller's Office generated a report from the SOR of all controlled and capitalized assets by agency. TS then used the discovery tool to detect all computers that were active on the City's network. Any computers that were turned off or disconnected from the network sixty days prior to when the tool was used could not be detected. The discovery tool generated a list of those assets and their serial numbers. This listing was matched to the corresponding records in the SOR. Only 7,000 of the approximate 9,000 IT assets detected by the discovery tool had a matching inventory record within the SOR. These assets were updated in the SOR to reflect TS as the asset custodian. There were some additional assets that had a record in the SOR but were not detected by the discovery tool and therefore remained on the agency asset custodians' inventory list and needed to be reconciled for the 2015 inventory.

**Reconciling Assets Found by the Discovery Tool**—Prior to assigning the remaining approximately 2,000 pieces of IT assets to TS within the SOR, TS and the Controller's Office attempted to determine the physical location of those assets with the help of the agency asset custodians. There are a variety of reasons why some assets were detected by the discovery tool but did not match the SOR. For example, 803 state-owned computers and the serial numbers on some computers did not match the SOR. City employees in the Department of Human Services and in the Office of Economic Development utilize these computers to conduct grant funded activities. As of March 2016, 815 other assets were not reconciled. The Controller's Office and TS suspect that hard drive replacements were completed without adjusting the record in the SOR as one of the reasons that 815 assets are not accurately accounted for in the SOR.

**Reconciling Assets Not Found by the Discovery Tool**—Some assets were not found by the discovery tool but remained in the SOR. For example, audit work found that sixty computers from one agency were disposed of by METech without certificates of destruction to support the disposal. The only evidence of disposal was an entry on a spreadsheet maintained by the agency. In addition, we found evidence of one stolen laptop that was not removed from the SOR. Because many of the IT assets are highly portable in nature, it is important to ensure that all disposals are documented as confidential and sensitive information is often on those types of devices.

According to the Standards for Internal Control in the Federal Government, promulgated by the U.S. Government Accountability Office:

> by not having quality information (current, complete, accurate, accessible, and provided on a timely basis), the auditee may not have the information necessary to support its internal controls surrounding the management of City assets. Internal controls are the plans, methods, policies, and procedures used to fulfill the mission, strategic plan, goals, and objectives of the entity. 4

---

GAO guidance specifies that internal controls around assets serve as the first line of defense in safeguarding assets and help managers achieve desired results through effective stewardship of public resources. Furthermore, in February 2014 Grant Thornton completed a review of the City’s IT Asset Management and recommended that TS conduct periodic reviews of IT asset inventory to ensure the accuracy and completeness of the IT assets and to help mitigate errors that are not in their immediate control.

The inability to reconcile approximately 800 IT assets and the lack of documentation for the disposed of assets demonstrates a need to improve upon inventory process controls to ensure an accurate inventory, minimize the loss of sensitive and confidential data, and maximize cost efficiency. Because of the portable nature of many IT assets, the Controller’s Office should work with TS to establish a base inventory for all 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.

**Agency Asset Custodians May Need Additional Communication and Training**

Audit work found that it would be beneficial to provide more detailed communications and additional training for the agency asset custodians regarding their role and responsibility of IT assets. We reviewed the email communication sent to the agency asset custodians about their role in the annual inventory process and about the transfer of IT assets to TS and determined the communication could have included more detail regarding the inventory process and the use of the discovery tool. This communication was critical to convey how the discovery tool impacts the agency asset custodian’s role in performing their annual inventory duties and the accuracy and efficiency of the inventory process.

The email contained instructions for agency asset custodians regarding their role in the inventory process. The email also contained a link to the 2015 Capital and Controlled Asset Inventory Reports (inventory report) for each agency, and three attachments—an asset inventory certification form (form), an inventory certification adjustment workbook (workbook), and the Computer Custodian Changes memorandum (memo)—to assist agency asset custodians with the annual inventory process.

Each agency’s inventory report listed the IT assets that were not identified by the discovery tool. Agency asset custodians were instructed in the email to physically locate the assets listed in the inventory report and document the disposition in the workbook. Documentation included any additions, deletions, or adjustments to asset information. However, the instructions failed to note the possibility that IT assets that appeared to be connected to the network (i.e., connected to the wall by an Ethernet cable) but had not been active for sixty days prior may not have been captured by the discovery tool and therefore should have appeared on the inventory report and would need to be updated in the SOR. The inventory process used in 2015 did not ensure an

---


6 In addition to the email communication, the Controller’s Office notified stakeholders in the Finance Officers Group and attendees of the Supervisors/Managers Meetings regarding the new asset management processes.
accurate listing of IT assets in the SOR. Enhancing communication to include more detailed information about nuances of the inventory process would ensure that there is a solid baseline inventory going forward, thereby maximizing the effectiveness of using the discovery tool in the future.

In addition, our audit work revealed that additional training is needed for agency asset custodians regarding the new inventory and asset management processes for IT assets. Specifically, not all agency asset custodians attended the mandatory training in 2015 to learn about the process to transfer and dispose of assets using the new electronic approach. We reviewed the training attendance form, which revealed that only 63 percent of agency asset custodians attended the training. The remaining agency asset custodians either attended one-on-one training or received no training at all. Because it is the responsibility of the Controller's Office to accurately report the City's financial information, which includes IT assets, they should ensure that those responsible for maintaining City assets attend mandatory training. According to the Standards for Internal Control in the Federal Government, an important element of internal control is providing staff with the right training and tools to ensure operational success. By not attending the mandatory training, some agency asset custodians may not have the necessary skills and understanding to take ownership of their respective assets and ensure that their asset inventory is accurate.

We also sought to determine whether agency asset custodians are prepared for future IT asset inventories by conducting a survey to assess their understanding of the new IT asset management process. The survey inquired about the inventory process and the previous training on the new automated asset transfer and disposal process. Survey results indicated that agency asset custodians are unclear on the new IT asset management process. Specifically, only 39 percent of agency asset custodians responded that the communication and training they received adequately prepared them for the new asset management process. Furthermore, multiple respondents indicated via an open-ended survey question that the current asset management process could be improved. Some respondents indicated that the related policies and procedures are not clear, a single point of contact was not available to assist with problem resolution during the transition, and communications about the process should be more frequent.

The Controller's Office sent a follow-up email to determine outstanding training needs. However, because this was a mandatory training they should have documented evidence that training was completed for all agency asset custodians. This would have allowed the Controller's Office to identify which agency asset custodians did not receive training to determine further training needs. Inaccurate reporting of IT assets can lead to a loss of IT assets, hinder the ability to budget for future IT equipment needs, present an increased fraud risk, and increase the potential for loss of sensitive and confidential City data. The Controller's Office and TS should 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 TS should ensure that the right person is in the agency asset custodian role annually and request the agency to assign a new custodian if needed.

**Information Technology Assets Waiting for Disposal Were Not Stored in a Secure Location**
The audit team found that the Technology Asset Purchasing Replacement Policy (Policy) does not specify a location for temporary storage of IT equipment and components that are designated for disposal. When an IT asset is no longer in use by an agency, the Policy specifies that the equipment must be disposed of securely. The City has contracted with METech Recycling to provide secure disposal, which consists of physical destruction of the device or wiping of the information that is stored on the device that will render it useless in accordance with best practices. Auditors determined that METech Recycling is a reputable company and historically has not experienced data loss through its operations. To prepare equipment and components for disposal, TS personnel remove hard drives from laptops and desktops. During a walk-through of the process, we observed that these components, including hard drives, computer system backup tapes, and CDs, were being stored in an unsecured location that is publicly accessible.

These hard drives and other data storage media should be secured in a locked or badged area until the disposal company representative retrieves them. The National Institute of Standards and Technology (NIST) specifies that care should be taken to ensure that all data contained on the devices has been removed or the device is destroyed and rendered unreadable. Confidential information or City data stored on computer hard drives and backups in publicly accessible areas is at risk of being accessed by unauthorized personnel, which could result in fines, security risks, or reputational damage. Due to the potential risk to the City, TS addressed this finding prior to the release of this report. We inspected the new storage location for disposal of equipment and confirmed that hard drives, computer system back-up tapes, and CDs are now secured behind a locked door.

The Chief Information Officer (CIO) in Technology Service 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 CIO IT Director of Service Operations should notify TS staff through a new policy about the establishment of the secure location.

Technology Services’ Existing Policy Needs to Be Updated

As part of our audit work, we reviewed the Policy, which provides guiding principles for the management of IT assets. The purpose of the Policy is to ensure that there is standardization for IT equipment through the City; that computers are adequately deployed to employees; and that TS is included in all purchasing decisions. We found that the Policy has not been updated recently and does not include procedures that reflect the new IT asset management process. Additionally, while the Policy documents the process for transferring unused IT assets, it does not provide clear, precise timeframes on when this is expected to be performed. Further, the Policy does not provide guidance for agencies in the event that IT equipment is lost or stolen.

---

7 NIST Media Sanitization Special Publication 800-88.
The Policy Is Outdated and Does Not Include Information Technology’s New Role Regarding Management and Oversight of IT Assets

We found that the Policy has not been updated since 2012 and, therefore, does not reflect the new IT asset inventory process. As a result, TS’s roles and responsibilities in the new process are not included. As previously mentioned, TS became the SOR custodian for all City computers at the time the electronic transfer and disposal process went live in 2015 and, going forward, the electronic discovery process will be used each year during the inventory process. These significant revisions related to roles and responsibilities and to the process should be included in the Policy.

Based on our assessment, we found that the new inventory process could benefit from more clearly documented and defined roles and responsibilities within the Policy. In an audit interview, TS personnel explained that they were still establishing their respective asset management roles and responsibilities as the custodian for IT assets. Establishing these roles and responsibilities will ensure that there is a common understanding of what is expected of various asset custodians throughout the process.

According to Standards for Internal Control in the Federal Government, management should design control activities such as policies, procedures, techniques, and mechanisms that enforce management’s directives to achieve the entity’s objectives and address related risks. As part of the control environment component, management defines responsibilities, assigns them to key roles, and delegates authority to achieve the entity’s objectives. Typically, an executive level manager, such as the Chief Information Officer or Chief Information Security Officer, reviews policies on a regular basis, which ensures that policies and procedures contain best practices and are in alignment with the organization’s objectives. If policies and procedures are not updated regularly or reflect the current environment, employees may not be fully aware of their responsibilities.

Procedures Related to Unused Information Technology Assets Need To Be Enhanced

In addition to updating the Policy to reflect TS’s new role as custodian of IT assets, the Policy can be strengthened in two different areas. First, the Policy is not clear enough regarding the expectation that agencies transfer unused IT assets back to TS. The language in the Policy encourages agencies to return unused equipment to TS for redeployment. However, it does not establish specific timeframes by which an agency must transfer back unused IT equipment. Accordingly, the Policy should be updated to clarify the objective of transferring unused equipment to TS for redeployment and the associated procedure should provide the steps for achieving the goal of transferring equipment.

---

8 Due to certain constraints, the Denver County Courts, Denver Public Library, and the District Attorney’s Office retained custodianship of computers. Denver International Airport and the Wastewater Management Division manage assets on systems outside of PeopleSoft and will also retain custodianship of all computers.

Second, the Policy does not provide guidance for agencies in the event that IT equipment is lost or stolen. TS currently has a separate internal procedure that outlines the procedure for loss or theft of equipment but agencies are not aware of the process. Further, the procedure does not include a step for notifying the Controller’s Office about the loss or theft so that the SOR can be updated accordingly. FAR 4.2 has an associated step-by-step procedure for asset transfer and disposal that includes a section on reporting lost or stolen assets, and the internal TS procedure is in line with this requirement.

Through our audit work, we found one instance of a stolen laptop that was misclassified as an active asset within the SOR. The IT Service Desk, a team within TS, was appropriately notified in accordance with the TS procedure about the stolen laptop and the police were also notified via a police report; however, the laptop was still listed in the SOR several months after it was stolen. According to TS’s loss or theft of equipment procedure, stolen equipment should be reported to the police and the IT Service Desk. However, the procedure lacks guidance about informing the Controller’s Office of lost or stolen equipment in order to update the SOR. Without this step in the procedure, the SOR will not be updated to reflect lost or stolen equipment and, therefore, the inventory will be inaccurate. Additionally, a stolen laptop or computer can contain valuable information, including personally identifiable information which can be used to steal someone’s identity or confidential City data. Therefore, TS’s loss or theft of equipment procedure should be updated to include a step to ensure that the SOR is updated appropriately and then the Policy should be updated to include the procedure.

12,000 assets were misclassified as computers.

Inaccurate Profile IDs Used To Update the System of Record

Our review of computer assets listed in the SOR revealed that some inaccurate profile IDs have been used to update the SOR. Through inspection of the Citywide SOR inventory report, we identified at least 12,000 assets that were misclassified as computers. Specifically, we found assets with descriptions indicating that the items were non-computer assets such as lawn equipment, furniture, and vehicles, yet the record in the SOR included a profile ID that is used for computers.

As a result of these misclassifications, assets have been incorrectly reported as IT equipment. As the City moves forward with the new inventory process, these misclassifications will affect the accuracy of the broader inventory. The review conducted by Grant Thornton recommended the completion of an asset data clean-up to ensure that information is correct and consistent in the SOR. To ensure accuracy and completeness of the City’s SOR, a clean-up should be performed on historical data. It is in the best interest of the Controller’s Office to ensure that IT assets are entered into the SOR accurately and the inventory is correct. Discrepancies and misclassifications make it difficult to perform an accurate analysis of IT assets.

In conclusion, policies provide guidance to establish the direction and tone for an agency, and include information on what is permitted or prohibited; procedures provide detailed and specific instructions for implementing the policy. Therefore, policies should be reviewed on a regular basis to ensure that they contain best practices and are in alignment with the organization’s objectives. If policies and procedures are not updated regularly or do not reflect the current environment, employees may not be fully aware of their responsibilities. Accordingly,
the CIO should review and update the Policy to ensure that it aligns with the new IT asset management process. The Policy should be updated to specify a timeframe by which agencies must transfer unused equipment back to TS for redeployment, establish a procedure for lost or stolen IT equipment that includes a control to update the system of record, and provide guidance on entering standardized asset descriptions and accurate profile IDs. In addition, the Policy should be reviewed annually.
RECOMMENDATIONS

We offer the following seven recommendations to improve the IT Asset Management process.

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.

**Auditee Response:** The Controller’s Office has been working with Technology Services on reconciling the asset listing for computers and laptops and this will continue through the 2016 annual inventory. Once the inventory is reconciled, it will be maintained through current business processes and inventoried annually. - 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.

**Auditee Response:** The Controller’s Office will provide training and communication to agency asset custodians prior to the 2016 inventory process. The Controller’s Office will communicate to agency leaders the importance of the agency’s responsibilities regarding asset management and ask that they verify their asset custodian(s) are the appropriate people assigned to this role. - June 30, 2016

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 IT Director of Asset Management should notify TS staff through a new policy about the establishment of the secure location.

**Auditee Response:** Technology Services (TS) has moved all equipment designated for disposal that may contain sensitive or City data to a secure location not accessible to the public. TS will develop and communicate a policy for IT Asset Management to include the establishment of the secure storage location. - October 31, 2016

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.

**Auditee Response:** Technology Services will create an IT Asset Management Policy and ensure that the new IT asset management process aligns with the policy. In addition, TS will define roles and responsibilities regarding IT asset management in the appropriate process documentation. - October 31, 2016
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 TS for redeployment.

**Auditee Response:** Technology Services will create an IT Asset Management Policy and specify a timeframe by which agencies must transfer unused equipment back to TS for redeployment. – October 31, 2016

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.

**Auditee Response:** Technology Services will establish a formal procedure for lost or stolen IT equipment that includes a control to update the system of record. – 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.

**Auditee Response:** We agree that the asset data should be as accurate as possible, however because the asset profile value does not impact reporting, tracking, inventorying, transferring, or disposing of any asset, this cleanup will be performed during our conversion to a new financial system. – June 2017
APPENDIX

Grant Thornton Audit

IT ASSET MANAGEMENT REVIEW

City of Denver - Technology Services

February 2014
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope and Procedures</td>
<td>1</td>
</tr>
<tr>
<td>Findings Summary</td>
<td>2</td>
</tr>
<tr>
<td>Proposed High Level Timeline</td>
<td>3</td>
</tr>
<tr>
<td>Short Term Action Items</td>
<td>5</td>
</tr>
<tr>
<td>Appendix A – Other Observations</td>
<td>8</td>
</tr>
<tr>
<td>Appendix B – IT Asset Management Process Maps</td>
<td>9</td>
</tr>
<tr>
<td>Appendix C – Pilot Results and Required Actions</td>
<td>12</td>
</tr>
</tbody>
</table>

© 2014 Grant Thornton LLP. All rights reserved.
Scope and Procedures

Grant Thornton was asked to review the current processes within the City of and County of Denver (‘City’) with a focus on Technology Services (‘Tech Services’) and assist in creating a plan to update Tech Services’ hardware asset inventory and inventory management practices. Grant Thornton spent two weeks onsite studying the current IT asset management practices of the City of Denver (City). This review was completed by performing the following:

• analyzing the prior asset management reports by the City’s Audit Services Division and Probar Associates
• reading the City’s Fiscal Accountability Rules and Fixed Asset Procedure
• conducting interviews and walkthroughs with City personnel including: Laura Haney, Scott Cardenas, Gene Humphries, Enier Ramirez, Vikki Robertson, Nick Nash, Linda Black, Valerie Wesley, Kris Dunmeyer, and Bill Brohl
• reviewing documentation including: annual physical asset lists, disposal reports, Windows 7 migration work papers, PSAM queries, asset category code reports, asset management forms, and FS asset integration diagrams
• reviewing asset management capabilities for both PeopleSoft and ServiceNow
• asserting IT asset management best practices for suitability
• validated process understanding and findings with relevant City personnel during review meetings

This initial review was designed to set the stage for further action by the City with an emphasis put on short term and impactful ‘wins’. The following report represents Grant Thornton’s core findings, high level timeline, short term action items, and other observations.
Findings Summary

The following concepts represent what we consider the most fundamental issues identified with the City’s IT Asset management program:

1) Current IT asset management program

An IT asset management program has several core components, each building on the other. The components in place define the maturity level and capabilities of that organization’s asset management program. These components are roughly defined as follows:

- **Inventory Management**
  - The Basic:  
  - What do we have on hand?

- **Configuration Management**
  - Define relationships and classes:  
  - Provides link to help desk

- **IT Asset Management**
  - Financial and lifecycle management

The City’s current stage is that of an incomplete inventory management program. The City has a capital asset management process which serves to capture and track all assets over a certain dollar threshold, but not a true IT inventory management process. Using the current workflow, PeopleSoft Asset Management system (PSAM) cannot currently capture and track any assets under $500 in value. The Controller’s Office has a draft policy update that will require the tracking of certain assets under $500 based on a risk determination. The current inventory management practices do not allow for assets such as mobile devices, IP connected devices, and leased assets under this $500 threshold. The City should implement this draft policy and bring the selected IT assets under $500 into the PSAM or other centralized asset management system.
2) IT asset management tools

The City currently uses PeopleSoft Asset Management to capture and track assets. PSAM is the core component of the PeopleSoft Enterprise Asset Lifecycle Management Suite. Also available as part of this suite are the IT Asset Management and Maintenance Management components, however, the City either does not utilize these last two components. It is within these last two components where the more mature IT asset management processes are found.

The City currently uses HEAT help desk software to handle purchase requests and track certain asset information. Information HEAT tracks includes asset information such as serial numbers, purchase requests, and issues; and user profile information including location, hardware, and software. HEAT does not integrate with PSAM. The lack of integration causes a potential for missing or incorrect data and prevents the City from utilizing the data to achieve cost reduction or operation efficiencies.

While the City is currently looking to install ServiceNow, the current system does not allow the City to adequately perform IT asset management, and only the most basic components of inventory management. The current systems do not allow the City to:

- capture adequate asset detail
- associate all IT assets with configurations, software, locations, or personnel
- eliminate paper and reduce manual entry errors
- monitor asset lifecycle
- monitor asset usage
- perform automated discovery and tracking of assets

3) IT asset management process failures

The current asset management processes and controls established and documented within City procedures are not consistently followed as evidenced in prior asset audits, interviews with City personnel, and review of current asset information. This issue, as much as the lack of adequate tools, has contributed to the inaccuracy of the asset inventories found by prior audits. While implementing additional controls would strengthen the process (and are outlined in a later section), consistently following the controls as designed would vastly improve the accuracy of the current asset inventory information that is captured. These missing or ineffective processes and controls include the following:

Asset information reviews:

- Form 55 for annual physical inventory of fixed assets is being filled out without a true physical inventory conducted
- disposed assets are reconciled versus Metech reports, however, no follow-up is done with discrepancies
- agencies are not filling out transfer documentation before moving assets
- asset tags are misunderstood and often wrong or missing
- purchasing category codes are misunderstood and often wrong

Proposed High Level Timeline
The proposed high level timeline ranges from short to long term actions with specificity decreasing as the timeline moves out. Additionally, time ranges are only a rough estimate as application implementation timeframes and resource considerations are unknown. The recommendations for short term remediation items are outlined in further detail in the following section.

Short Term (3-6 m)
- Physical inventory
- Asset data clean-up
- Retain personnel on current processes
- Add periodic reviews
- Reduce manual data entry
- Other minor process changes
- Expand processes to the rest of Tech Services

Medium Term (6-18 m)
- Redefine IT asset scope
- Implement new asset management tools (e.g. ServiceNow)
- Capture expanded asset detail
- Tee assets to users
- Tie in with help desk use
- Combine with software regis
- Implement asset configuration management
- Roll out processes to other agencies

Long Term (12-36 m)
- Centralize IT asset management and authority
- Implement automated discovery techniques
- Monitor asset usage
- Monitor asset lifecycles
- Inventory planning and procurement forecasting
- Compliance tracking

As the IT asset management program matures through this timeline, the program’s value and purpose will change as it moves from inventory management, to configuration management, to true IT asset management.
Short Term Action Items

The following short term action items represent the steps we believe are required to fix Tech Services asset inventory and control the accuracy and completeness of the asset inventory going forward. These steps are focused on what can be achieved now using current systems and personnel.

1) Physical inventory

Conduct a physical inventory in conjunction with the asset data clean-up. The physical inventory at each agency is the most vital step the City must perform in order to correct the current IT asset inventory.

We recommend that the City start with a pilot asset group from within Tech Services, and perform the following procedures both in PSAM and within the department need to be:
- physically identify each asset
- reconcile PSAM description and model #
- verify and document location code
- reconcile serial number and asset tag
- review asset status
- review organization and accompanying details

Submit the physical inventory changes via Form 55 to have updates applied to PSAM. Asset changes for location code, serial number, and asset tag should be updated by the agency asset custodian. These changes do not need to be input onto the Form 55.

For missing or extra assets found, complete the following:
- for assets (disposed) on the Asset log which still remain in PSAM, create an explanatory memo and have it signed by the Expending Authority so that it can be removed from PSAM
  - this can be done in batches with multiple items on each memo
- for assets found that are not in PSAM, submit an asset input form and asset acquisition information to add the asset to PSAM
- for transferred assets found remaining on Tech Services’ inventory, submit a Form 11GS for each asset to be moved to the correct agency’s inventory
2) Asset data clean-up

Update the data within PSAM based on the results of the physical inventory and information gathering process. In addition to the asset information being correct, the information needs to be consistent. This means making sure that descriptions, model #, locations, address, etc., are all entered in the same manner. Correct and standardize details that are missing or otherwise insufficient within the system. Identify and remove duplicate assets.

The forms used to update asset details described in the Physical Inventory section could be used along with a master change list for the Controller’s Office to update asset details, or alternatively access to make updates could be granted to Tech Services personnel.

3) Retrain personnel on current processes

For each of the IT asset management process failures listed previously, some retraining is needed. Conduct periodic training for all personnel that install, move, add, change or are otherwise involved in the IT asset management process. Additionally, creating procedural or reference documentation will aid in the consistency of processes such as purchasing category code usage. Each of the following finding topics should be covered by the asset management training:

- asset tags are misunderstood and often wrong or missing
- purchasing category codes are misunderstood and often wrong
  - a ‘cheat sheet’ of common asset types with corresponding category codes would help to drive consistency in this process
- disposed assets are reconciled versus Metech reports, however, no follow-up is done with discrepancies
- agencies are not filling out transfer documentation before moving assets
- updating missing or extra assets found (see Physical inventory section)

4) Add periodic reviews

To ensure the accuracy and completeness of Tech Services IT asset inventories, several periodic reviews should be added to the existing asset management procedures. These reviews will also help to mitigate errors in asset management outside Tech Services’ control. The following proposed reviews should be performed by the Asset Manager:

- weekly or monthly review of new assets
  - this would include reviewing both asset existence and detail
- monthly or quarterly review for duplicate assets
- weekly or monthly review of disposed assets

These reviews should be started weekly and then transitioned to monthly as the processes become more stable. The City should also consider performing physical inventories on certain asset classes more often if they are found to require a large correction during each audit. Each review will require the Asset Manager to make the appropriate updates to PSAM.
5) Reduce manual data entry

The current asset management process requires multiple manual entries for each asset. Each entry represents a potential point of failure. Based on our review of prior audit findings, we know this to be an issue. While a fully integrated system is not in our short term plan, any manual data entry that can be eliminated is beneficial. The largest potential to remove manual data entry is when new computer hardware is entered by Tech Services. For common vendors such as Dell, an electronic solution for sending and capturing asset detail (i.e. serial number) should be arranged. While not all vendors may be able to provide this data electronically, several of these repeat vendors make up a large percentage of assets and therefore data entry.

6) Other minor process changes

These are several minor process changes that should be implemented in conjunction with the initial review of a single asset class. These current minor process changes include the following:

- add follow up to disposal process where updates are made to PSAM when proper forms are missing
- ensure that assets are entered into PSAM before they are deployed
  - large orders that come in multiple deliveries must be managed so that assets are not physically deployed prior to being entered into PeopleSoft
  - validate that orders with duplicate assets have serial numbers matched with where they are deployed
- ensure that the Tech Services IT Asset Manager has the PSAM logical access required to pull reports and make approved edits

7) Expand inventory and data clean up to all of Tech Services

After the conclusion of the pilot, document the lessons learned and update the full process. Roll out the updated process to all IT hardware asset classes within Tech Services in a method that resources will allow.
Appendix A – Other Observations

The following list represents, in no special order, other observations not included in detail elsewhere in the report:

- the current IT asset management groups have no authority to move or redeploy assets from other agencies
- IT asset details are not readily available to help desk personnel
- there is not a centralized IT asset management group for the City
- the IT asset management group has separate functions for hardware and software
- IT assets are not tied to individuals
- the configuration of IT assets is not tracked
- the software associated with IT assets is not tracked
- there is no automated and persistent inventory discovery tool
- current tools do not capture and track IT asset lifecycles
Other Process Controls

Legend
- Control updates
- Potential process redesign

Periodic review for duplicate assets (STAI #4)

PSAM

Periodic physical review and update of asset location, status, etc via Form SS and 13G5. (STAI #4)

User to Asset Tracking

User to asset tracking:
TS Admns manually update user and asset info when new hires, transfers, moves, or removals occur

User to asset tracking (from New Assets process):
If computer deployment, user information is sent to TS Admns for tracking
Appendix C – Pilot Results and Required Actions

Grant Thornton completed a physical inventory for workstation, laptop, and tablet computer assets within Tech Services. We compared each of these inventoried assets to a current PeopleSoft Asset Management listing for Tech Services. An analysis over the assets not found during the physical review was completed to identify the correct action to be taken for each asset. This analysis used Active Directory, SCCM, and PeopleSoft data sources to link asset serial numbers to computer name, asset ID, tag number, and location information. Based on this analysis, the City will need to complete several steps to clean-up and transfer these assets.

Summary of findings
The Controller’s Office provided an asset inventory from PeopleSoft Asset Management that included 4,230 total Tech Services capital and controlled computer assets. During the physical inventory, 512 assets were found and documented, leaving 3,718 assets on Tech Services inventory not found. We found two of 24 capital assets during the physical review, and did not identify any proposed changes based on our analysis. These remaining 32 items will require further investigation. The results of our analysis of the approximately 4,000 controlled assets not found is as follows:

- 115 assets were disposed but not removed from inventory
- 2224 assets were identified for transfer to another agency
- 1526 assets were not located during the physical inventory and we were unable to identify the proper agency to transfer the asset to

Inventory action items
The following procedures are required to complete the scrub of Tech Services computer asset inventory.

1. Issue: Assets found during physical inventory not on inventory listing from PSAM

   The assets located during the physical inventory that did not appear on the Tech Services inventory list from PSAM, generated by the Controller’s Office, were identified and documented in Physical Inventory Not on Controller’s List.xlsx. Each of the assets was categorized by the agency’s inventory in which the asset was most likely to appear based on tag #, computer name, and/or location.

   Resolution: Assets physically located during the inventory will need to be located on the suggested agencies inventory and moved to Tech Services inventory listing per the Physical Inventory Not on Controller’s List.xlsx. For any assets that are not located in PSAM, an asset input form including asset acquisition information will be submitted to update PSAM. For those assets that did not have a unique identifier linking them to an agency additional research may be required to determine which inventory list they are associated with. Once identified the asset will need to be transferred to Tech Services. If the asset cannot be located then an asset acquisition form will be required to ensure that all items identified in the physical inventory have been accounted for.
2. **Issue: Assets incorrectly disposed**

   There were four assets identified in the physical asset inventory that appear on the Retired Controlled Assets tab of the Tech Services inventory list generated by the Controller’s Office. See Controller T5 Asset List with Found Assets Highlighted.xlsx.

   **Resolution:** These four assets should have a Form 55 created to have updates applied to PSAM to ensure that they are not listed as retired and are included in the current physical inventory.

3. **Issue: Disposed assets not removed from inventory**

   There were 115 assets identified that appear on disposal listings, but still remain on Tech Services inventory. These assets are documented in Assets not found - Analysis.xlsx within the DISPOSED tab will need to be removed from the inventory listing within PSAM.

   **Resolution:** For this list of assets, create an explanatory memo and have it signed by the Expending Authority so that it can be removed from PSAM.

4. **Issue: Assets not physically located requiring transfer to other agencies**

   There were 2,324 assets not physically located but identified for transfer to another agency. Each of the assets was categorized by the current Agency based on a unique identifier in the tag #, computer name, and/or location. These assets are listed in worksheets by agency in Assets not found - Analysis.xlsx within the green tabs starting with LIBRARY and ending with SAFETY OTHER. All agencies within the GOV and Safety domains have a tab represented. The SAFETY OTHER items may need to be investigated further to identify the appropriate Safety sub-domain.

   **Resolution:** For each of the colored worksheet tabs, a Form 13GS must be created to move the assets to the correct agency’s inventory listing within PSAM.

5. **Issue: Unable to physically locate, confirm disposal or associate with another agency**

   There were 1,526 assets for which we were unable to validate resolution as they were not associated with another agency or disposed of. These assets are listed in Assets not found - Analysis.xlsx within the green UNKNOWN tab. Additionally, we were unable to locate the 52 capital assets included on the inventory listing and as such these will require further investigation. These assets are listed in Assets not found - Analysis.xlsx within the Capital Assets Not Found tab.

   **Resolution:** Each of these assets will need to be investigated to determine proper resolution. Both citywide PeopleSoft inventory and HEAT manual searches may identify the proper location for these assets.
April 7, 2016

Auditor Timothy M. O’Brien, CPA
Office of the Auditor
City and County of Denver
201 West Colfax Avenue, Dept. 705
Denver, Colorado 80202

Dear Mr. O’Brien,

The Office of the Auditor has conducted an audit of IT Asset Management.

This memorandum provides a written response for each reportable condition noted in the Auditor’s Report final draft that was sent to us on March, 18, 2016. This response complies with Section 20-276 (c) of the Denver Revised Municipal Code (D.R.M.C.).

AUDIT FINDING 1
Weaknesses Exist with the City’s Process for Managing Information Technology Assets

RECOMMENDATION 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 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.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>September 30, 2016</td>
<td>Jessica Chandler 720-913-5223</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.1
The Controller’s Office has been working with Technology Services on reconciling the asset listing for computers and laptops and this will continue through the 2016 annual inventory. Once the inventory is reconciled, it will be maintained through current business processes and inventoried annually.
### RECOMMENDATION 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.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>June 30, 2016</td>
<td>Kelli Bennett 720-913-5156</td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 1.2**
The Controller’s Office will provide training and communication to agency asset custodians prior to the 2016 inventory process. The Controller’s Office will communicate to agency leaders the importance of the agency’s responsibilities regarding asset management and ask that they verify their asset custodian(s) are the appropriate people assigned to this role.

### RECOMMENDATION 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.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>Workday Financials go-live June 2017</td>
<td>Kelli Bennett 720-913-5156</td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 1.7**
We agree that the asset data should be as accurate as possible, however because the asset profile value does not impact reporting, tracking, inventorying, transferring, or disposing of any asset, this cleanup will be performed during our conversion to a new financial system.
Please contact Kelli Bennett at 720-913-5156 with any questions.

Sincerely,

Beth Machann
City Controller

cc: Brendan Hanlon, Chief Financial Officer
    Kelli Bennett, Director Accounting & Financial Reporting
    Jessica Chandler, Financial Manager
    Kip R. Memmott, MA, CGAP, CRMA, Director of Audit Services
    Shannon Kuhn, CISA, IT Audit Supervisor
April 8, 2016

Auditor Timothy M. O’Brien, CPA  
Office of the Auditor  
City and County of Denver  
201 West Colfax Avenue, Dept. 705  
Denver, Colorado 80202  

Dear Mr. O’Brien,

The Office of the Auditor has conducted an audit of IT Asset Management.

This memorandum provides a written response for each reportable condition noted in the Auditor’s Report final draft that was sent to us on March 18, 2016. This response complies with Section 20-276 (c) of the Denver Revised Municipal Code (D.R.M.C.).

**AUDIT FINDING 1**  
Weaknesses Exist with the City’s Process for Managing Information Technology Assets

**RECOMMENDATION 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 IT Director of Asset Management should notify TS staff through a new policy about the establishment of the secure location.

| Agree or Disagree with Recommendation | Target date to complete implementation activities  
(Generally expected within 60 to 90 days) | Name and phone number of specific point of contact for implementation |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>10/31/2016</td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 1.3**  
Technology Services (TS) has moved all equipment designated for disposal that may contain sensitive or City data to a secure location not accessible to the public. TS will develop and communicate a policy for IT Asset Management to include the establishment of the secure storage location.
RECOMMENDATION 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.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>10/31/2016</td>
<td>Stephen E. Coury 720-913-4919</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.4
Technology Services will create an IT Asset Management Policy and ensure that the new IT asset management process aligns with the policy. In addition, TS will define roles and responsibilities regarding IT asset management in the appropriate process documentation.

RECOMMENDATION 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 TS for redeployment.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>10/31/2016</td>
<td>Stephen E. Coury 720-913-4919</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.5
Technology Services will create an IT Asset Management Policy and specify a timeframe by which agencies must transfer unused equipment back to TS for redeployment.
**RECOMMENDATION 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.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>10/31/2016</td>
<td>Stephen E. Coury 720-913-4919</td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 1.6**
Technology Services will establish a formal procedure for lost or stolen IT equipment that includes a control to update the system of record.

Please contact Stephen E. Coury at 720-913-4919 with any questions.

Sincerely,

Scott Cardenas
Chief Information Officer

cc: Kip R. Memmott, MA, CGAP, CRMA, Director of Audit Services  
Shannon Kuhn, CISA, IT Audit Supervisor  
Brendan Hanlon, Chief Financial Officer  
Beth Machann, Controller  
Kelli Bennett, Director Accounting & Financial Reporting  
Jessica Chandler, Financial Manager  
Alex Stefanacci, IT Director of Service Operations  
Stephen E. Coury, Chief Information Security Officer