Mayor

Betsy Price

Council Members

Carlos Flores, District 2

Brian Byrd, District 3

Carry Moon, District 4

Gyna Bivens, District 5

Jungus Jordan, District 6

Dennis Shingleton, District 7

Kelly Allen Gray, District 8

Ann Zadeh, District 9

Information Technology (IT) Asset Verification Audit

August 4, 2017

City of Fort Worth
Department of Internal Audit

200 Texas Street
Fort Worth, Texas 76102

Audit Staff

Patrice Randle, City Auditor
Terry Holderman, Assistant City Auditor
Sam King, IT Programmer/Analyst II

The Information Technology (IT) Asset Verification Audit was conducted as part of the Department of Internal Audit's Fiscal Year 2016 Annual Audit Plan.

Audit Objective

The objective of this audit was to confirm the physical existence or proper disposition of assets purchased by and belonging to the City of Fort Worth.

Audit Scope

Our audit scope covered IT assets purchased by purchase order and/or procurement card, and IT assets that were decommissioned during FY2015 and FY2016.

Opportunities for Improvement

Enhanced accountability for IT assets

Written policies and procedures

Executive Summary

As part of our 2016 Annual Audit Plan, the Department of Internal Audit conducted an Information Technology (IT) Asset Verification Audit of IT assets purchased by the City of Fort Worth.

When testing for the accountability of decommissioned assets, the Department of Internal Audit utilized three sets of data to identify City IT assets.

- Discovery Tool – for IT assets that had been connected to the City of Fort Worth's network.
- BuySpeed On-Line (the City's procurement software) – for IT assets purchased through the City's procurement process.
- Procurement card transactions – for IT assets purchased with a City-issued procurement card.

By utilizing the City's Discovery Tool software and procurement sources, the Department of Internal Audit was able to locate and verify the physical existence of each sampled asset currently in use by City staff.

During our audit, we were able to verify the disposition of 127 of 130 decommissioned IT assets included in our sample. The Department of Internal Audit could not verify the proper disposition of one IT asset because there was no serial number to confirm that the decommissioned asset belonged to the City of Fort Worth. The other two IT assets could not be verified because they were not located on the manufacturer's/contracted vendor's end-of-life asset listing.

The Discovery Tool software can effectively track IT assets that have the Discovery Tool client software installed and have been logged onto the City's network. However, if Discovery Tool detects that an IT asset has not been logged onto the network over a specific period of time, there is a lack of communication between ITS and the user department to ensure accountability for that particular asset.

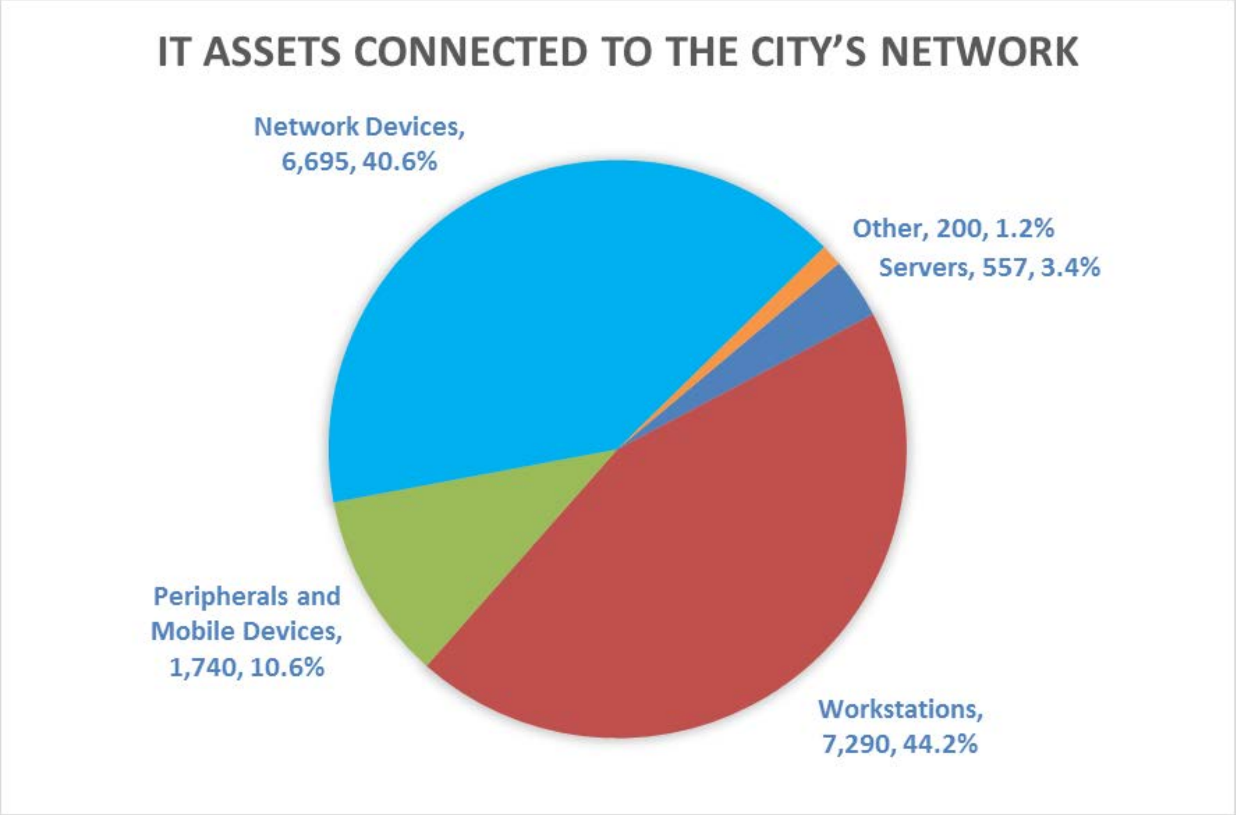
We concluded that there are no written policies and/or procedures to help ensure that IT assets are properly accounted for throughout the City.

Our audit findings are discussed in more detail within the Detailed Audit Findings section of this report.

Table of Contents

Background

The Information Technology Solutions Department (ITS) is responsible for maintaining an inventory of IT assets (such as mobile devices, servers, workstations, peripherals and network devices, etc.) acquired with City funds. As documented in the following chart, the City of Fort Worth (CFW) had over 16,000 IT assets connected to the City's network as of September 16, 2016. Laptops and desktops (noted as Network Devices and Workstations within the chart) account for approximately 85% of these assets.



Source: Discovery Tool Software

ITS uses the Discovery Tool software to track IT assets and to provide information about personal computers and other IT assets into a centralized database. The Discovery Tool software detects IP-addressable hardware (including servers, desktops, laptops, network printers, switches and devices) and software connected to the City's network. It also has the ability to autonomously identify new assets being added to the network and can track hardware, software and configuration changes. When IT assets are received, ITS personnel install software (if applicable) and assign an asset number for each asset received. Such action allows the asset to be identified by the Discovery Tool software once the asset is attached to the City network.

For decommissioned assets, City policy requires that ITS personnel remove data and software before the assets are returned to the manufacturer. Once the City's asset tag number and CFW information is removed, the asset is returned to the manufacturer. The manufacturer sells the asset and provides documentation supporting auction proceeds. The manufacturer also sends a check in the amount received from the auction, along with corresponding asset serial numbers.

IT assets are assigned to user departments for the purpose of conducting City business. ITS staff indicated that it is the departments' responsibility to retain records of the IT asset assignments.

Objective

The objective of this audit was to confirm the physical existence or proper disposition of IT assets purchased by and belonging to the City of Fort Worth.

Scope

Our audit scope covered IT assets purchased by purchase order and/or procurement card, and IT assets that were decommissioned during FY2015 and FY2016.

Methodology

To achieve the audit objectives, the Department of Internal Audit performed the following:

- obtained IT asset information from the Discovery Tool software;
- verified the existence of IT assets by conducting physical observations in user departments;
- reviewed purchase card transactions for IT asset purchases;
- conducted interviews with IT personnel;
- reviewed end-of-life and other departmental documentation; and,
- evaluated internal controls related to IT assets.

We conducted this audit 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.

Audit Results

The Department of Internal Audit determined that the CFW has incident and installation documentation to support new, replaced, and decommissioned IT assets. During our audit, we were able to verify the existence of each sampled IT asset that was currently in use by City staff, and were able to account for 127 of 130 IT assets that had been decommissioned after reaching the end of their useful life. During the audit, ITS staff was able to provide requested information in a timely manner to help facilitate our asset verification efforts.

IT Assets Currently in Use
While the Discovery Tool software and departmental inventory listings help ensure accountability for IT assets, we concluded that better communication (between ITS and user departments) is required to help ensure that anomalies identified during the Discovery Tool software runs are resolved in a timely manner.

End-of-Life IT Assets
ITS spreadsheets, entitled Request for Disposition, are used to document end-of-life assets that have been returned to the manufacturer/contracted vendor for proper disposition. Request for Disposition spreadsheets include information such as asset model, serial and City asset tag number. To verify proper disposition of the City's end-of-life IT assets, the Department of Internal Audit selected Request for Disposition spreadsheets for the months of March and November 2015. We then randomly selected 56 sample items from the March spreadsheet and 74 from the November spreadsheet.

- The process for decommissioning end-of-life assets is initiated upon user departments' requests via Information Technology Service Management (ITSM) tickets. Since ITSM information is documented onto Installation Delivery Signature Sheets (which contain signatures of the user department and the assigned ITS technician), December 2014 through March 2015 Installation Delivery Signature Sheets were reviewed to support the March 2015 Request for Disposition.

  The Department of Internal Audit successfully located 30 of the 56 (53.6%) end-of-life March sample items. It should be noted that since Installation Delivery Signature Sheets are scanned as images, the Department of Internal Audit had to manually/visually inspect scanned images, which was very tedious and prone to human error. While we did not observe Installation Delivery Signature Sheets supporting the remaining 26 decommissioned assets, we were able to verify the existence of those assets by reviewing Dell Inc.'s end-of-life asset listing. An example of the CFW's Installation Delivery Signature Sheet is at Exhibit I of this report.

- Due to the level of difficulty in searching Installation Delivery Signature Sheets for the March sample, the Department of Internal Audit chose to compare asset serial numbers on ITS' spreadsheet to those noted on Dell's end-of-life asset listing for the November sample. Based on our audit results, three exceptions were noted.

  ➢ One asset could not be positively verified because there was no serial number to be compared. For example, ITS' spreadsheet indicated that the serial number had been removed from the asset, prior to being received in ITS for decommissioning. The Department of Internal Audit was, therefore, unable to conclude as to whether the decommissioned asset actually belonged to the City.

- Serial numbers for two other assets could not be traced to Dell's end-of-life asset listings made available to Internal Audit.

Policies and Procedures

In reference to policies and procedures, the City currently has regulations that address the security of IT assets (i.e., responsibility for negligent or malicious acts that negatively affect the confidentiality, integrity or availability of an IT asset). However, there are no written policies and/or procedures to help ensure that IT assets are properly accounted for throughout the City.

Overall Evaluation

High	Medium	Low
Lack of full accountability for IT assets		
	No written policies and procedures	

Detailed Audit Findings

1. **There is no full accountability of IT assets purchased by the City of Fort Worth.**

The Discovery Tool software identifies City-owned IT assets that are loaded with the Discovery Tool client software and connected to the City's network. While the software helps ensure accountability for IT assets, the City's utilization of information provided by this software does not maximize asset accountability. For example, if Discovery Tool indicates that a specific laptop was connected to the City's network from January 1st through May 5th, but did not connect to the City's network from May 6th through December 31st, there is no follow-up with the applicable department to verify that the laptop (which is not at its end of life) still exists.

Most City departments maintain a listing of IT assets purchased by and/or assigned to their department. However, when Discovery Tool detects an asset during one software run, but does not detect that same asset during a subsequent run(s), there is no follow-up with the user department. As a result, there is an increased risk of theft, abuse and/or misuse. The time in which an IT asset did not connect to the City's network could signify the asset is no longer being used, or it could signify that the asset was stolen, being used for personal use, etc.

When comparing Discovery Tool records to three (3) user departments' inventory listings, the Department of Internal Audit identified 19 instances where an IT asset had once been identified by the Discovery Tool software, but was not included in the departments' inventory listings. Audit observations were, therefore, made to verify the existence of those 19 assets. Based on our observations, all 19 assets were physically observed. It should be noted that not all departments are capturing asset serial numbers in their inventory listings. Departments are capturing asset descriptions and City asset tag numbers, which were used to verify the existence of some assets.

On June 16, 2017, the Department of Internal Audit compared Discovery Tool and departmental records. We identified IT assets noted as not being connected to Discovery Tool since December 2016. However, the IT assets had been connected to the City's network subsequent to December 2016 and were in use as of June 2017.

The Discovery Tool only includes CFW IT assets purchased through ITS. The CFW recently implemented a process whereby all IT-related purchases must be approved and scheduled through an ITSM ticket. Internal Audit commends management for choosing to implement this process as it will enhance the City's accountability for IT assets.

It should be noted that as a part of the City's budgeting process, ITS staff prepare a list of desktops, laptops, etc. eligible for replacement/refresh. Per ITS, during this process, variances are identified and corrections are made to ITS records prior to processing refresh orders. If there is additional information, that information is verified against procurement data and then incorporated into the annual refresh program.

The Government Finance Officers Association (GFOA) lists adequate care as a best practice related to maintaining control over items that are not capitalized. Such care helps ensure that adequate control is maintained over any such items that fall within three categories, one of which is items that require special attention to compensate for a heightened risk of theft ("walk-away" items). Examples would include assets that are both easily transportable and readily marketable or easily diverted to personal use such as laptops, desktops, monitors and printers.

Recommendation 1A: *The Chief Technology Officer should require that ITS identify anomalies that are identified during routine Discovery Tool software runs. Any anomalies, not resolved by ITS, should be communicated to user departments for discrepancy resolution.*

Auditee's Response: Concur. A project is currently underway to replace Discovery Tool with a robust asset tracking system to manage the technology assets. Purchase and implementation of the system will begin in January 2018 and completed by October 2018.

Target Implementation Date: January 2018

Responsibility: Chief Technology Officer

Recommendation 1B: *The Chief Technology Officer, in conjunction with the Chief Financial Officer, should consider configuring PeopleSoft to require that purchases of IT equipment be systematically routed through the Information Technology Solutions Department for approval, prior to the procurement.*

Auditee's Response: Concur. ITS worked with Purchasing to require ITS approval of technology purchases.

Target Implementation Date: Complete.

Responsibility: Chief Technology Officer

Recommendation 1C: *The City Manager should require that departments maintain departmental IT inventory listings which should include, at a minimum, asset descriptions, City asset tag numbers, asset serial numbers, assigned user, locations and should be used to help resolve discrepancies identified during Discovery Tool runs (i.e., a computer once detected by the Discovery Tool software is not decommissioned, but has not been detected by Discovery Tool in several weeks or months).*

Auditee's Response: Partially Concur. Management recognized responsibility for managing computer assets was divided between the Departments and ITS. Departments funded computer purchases through their operating budget and managed the physical computer asset. ITS managed the software components through the Discovery Tool. Beginning in FY17, funding for the procurement of computer assets was consolidated in the Computer Equipment Replacement Fund managed by ITS. Going forward, ITS will coordinate with Departments to manage the funding; the physical asset (including the asset identifying information listed above); and the software components for computer assets.

Target Implementation Date: January 2018

Responsibility: Chief Technology Officer

2. No written City-wide policies and procedures exist to govern the CFW's IT inventory.

The CFW has no written policies and procedures to govern the City's IT asset inventory process, or guidance regarding IT asset inventory management and/or disposal. Without documented policies and procedures, the authority and responsibility of employees involved in the inventory process may be unknown and/or unclear, and the risk of loss, theft or misappropriations of IT assets is increased.

During our audit, we identified information technology security policies (Administrative Regulations D5) established for the protection (i.e., confidentiality, integrity, etc.) of IT assets. However, no written city-wide policies related to proper inventorying and accountability.

Within GFOA's recommended best practices, communication is noted as an essential component of a comprehensive framework of internal controls. One method of communication that is particularly effective for controls over accounting and financial reporting, per GFOA, is the formal documentation of accounting policies and procedures. A well-designed and properly maintained system of documenting policies and procedures enhances both accountability and consistency. The resulting documentation can also serve as a useful training tool for staff.

During our audit, ITS indicated that there is no geolocation software or radio-frequency identification (RFID) tagging of IT assets to track their finite locations. Each department is, therefore, responsible for retaining records of the specific asset assigned to each employee/purpose, since assets can move from office to office and/or from site to site. Based on our inquiries, all departments may not be aware of such requirements, as not all departments maintain their own departmental IT asset inventory listing.

Recommendation 2: *The Chief Technology Officer should ensure that policies and procedures related to the City's IT inventory are documented within the departmental and city-wide policies and procedures. Any changes in policy and procedures that occur between periodic reviews should be promptly updated as those changes occur.*

Auditee's Response: Concur. ITS will work with Purchasing to ensure departmental procurement and operating procedures are updated as the new inventory system is implemented.

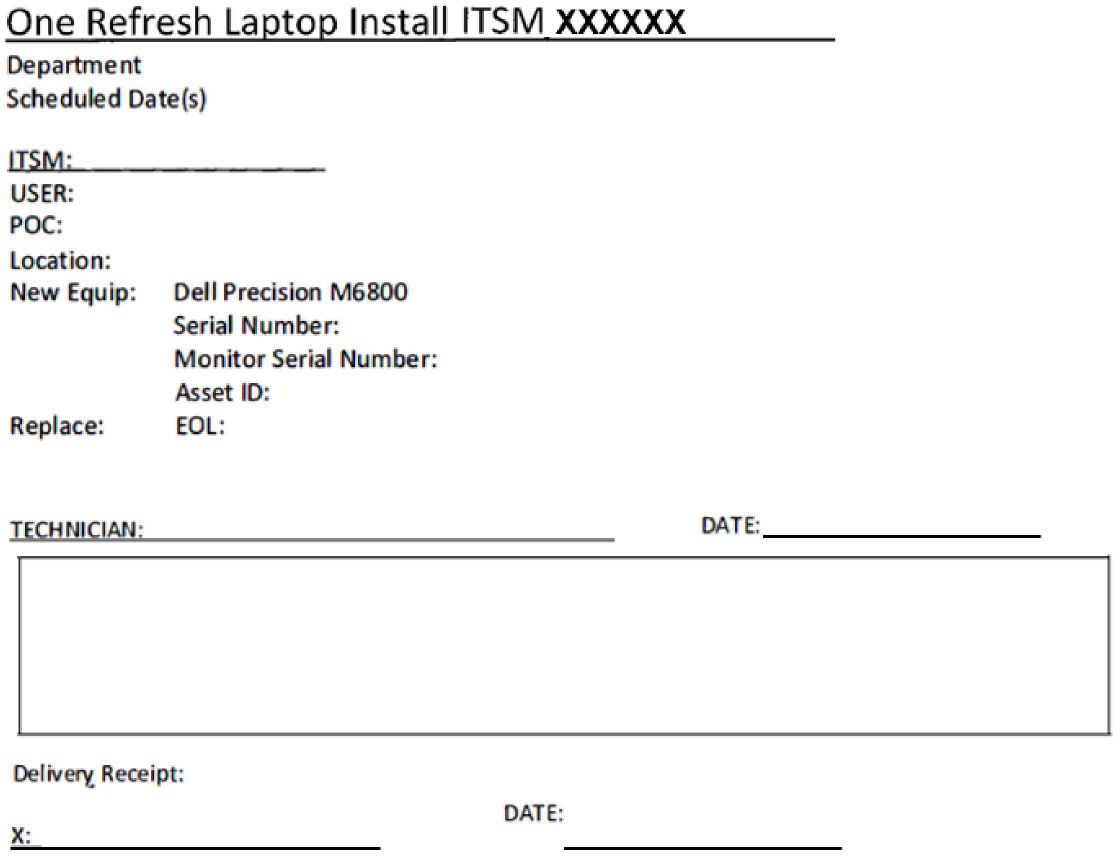
Target Implementation Date: January 2018

Responsibility: Chief Technology Officer

Acknowledgements

The Department of Internal Audit would like to thank all City departments for their cooperation and assistance during this audit.

Exhibit I – CFW Installation Delivery Signature Sheet



One Refresh Laptop Install ITSM XXXXXX

Department
Scheduled Date(s)

ITSM: ______________

USER:

POC:

Location:

New Equip: Dell Precision M6800
Serial Number:
Monitor Serial Number:
Asset ID:

Replace: EOL:

TECHNICIAN: ______________________________ DATE: ______________________

Delivery Receipt:

X: ______________________________ DATE: ______________________