A Report to the
Citizens of Salt Lake County
The County Mayor and the
County Council

An Audit of the Salt Lake County Information Technology Division

OFFICE OF THE
SALT LAKE COUNTY
AUDITOR

SCOTT TINGLEY
COUNTY AUDITOR

February 2021

An Audit of the Salt Lake County Information Technology Division

February 2021

Scott Tingley, CIA, CGAP
SALT LAKE COUNTY AUDITOR

Cherylann Johnson, MBA, CIA, CFE, CRMA
CHIEF DEPUTY AUDITOR

Shawna Ahlborn
AUDIT SERVICES DIVISION ADMINISTRATOR

AUDIT MANAGER:
Colleen Hilton

AUDIT STAFF:
David Lewis, CPA, CIA, CFE, CMA

OFFICE OF THE SALT LAKE COUNTY AUDITOR
AUDIT SERVICES DIVISION

OUR MISSION

To foster informed decision making, strengthen the internal control environment, and improve operational efficiency and effectiveness for Salt Lake County, through independent and objective audits, analysis, communication, and training.

SCOTT TINGLEY
CIA, CGAP
Salt Lake County Auditor
STingley@slco.org

CHERYLANN JOHNSON
MBA, CIA, CFE
Chief Deputy Auditor
CAJohnson@slco.org

ROSWELL ROGERS
Senior Advisor
RRogers@slco.org

STUART TSAI
JD, MPA
Property Tax
Division Administrator
STsai@slco.org

SHAWNA AHLBORN
Audit Services
Division Administrator
SAhlborn@slco.org

OFFICE OF THE
SALT LAKE COUNTY
AUDITOR
2001 S State Street, N3-300
PO Box 144575
Salt Lake City, UT 84114-4575

(385) 468-7200; TTY 711
1-866-498-4955 / fax

February 19, 2019

Honorable Members of the Salt Lake County Council,
Honorable Salt Lake County Mayor, and
The Citizens of Salt Lake County

Re: An Audit of the Salt Lake County Information Technology Division

The Salt Lake County Auditor's Audit Services Division has completed *An Audit of the Salt Lake County Information Technology Division*. The purpose of the audit was to evaluate the IT Division's internal controls to determine if service contract revenue is billed and collected according to the terms of the service contract agreements, if purchases and expenditures are properly authorized and records are complete and accurate, and if adequate safeguards are in place to protect County assets and resources. A detailed report of the audit objectives, conclusions, findings, and recommendations follows this letter. An executive summary of the audit report can be found on page 1.

By its nature, this report focuses on issues, exceptions, findings, and recommendations for improvement. The focus should not be understood to mean that we did not find various strengths and accomplishments. We truly appreciate the time and efforts of the IT Division staff throughout the audit. Our work was made possible by their cooperation and prompt attention given to our requests.

We would be happy to answer any questions you may have about the audit or the findings and recommendations contained in this report.

Sincerely,

Scott Tingley, CIA, CGAP
Salt Lake County Auditor

Other recipients of this report:
Megan Hillyard, Department Director, Department of Administrative Services
Zachary Posner, Chief Information Officer
Cherie Root, Associate Division Director – Finance and Administration, IT Division
Kimball Ball, Administrative and Fiscal Manager, IT Division

Table of Contents

Executive Summary

Background and Purpose

We recently completed an audit of the Salt Lake County Information Technology Division. The Information Technology Division provides a broad range of information technology related services for all County offices, departments, and divisions. As an integral part of County operations, IT is responsible for ensuring that the County's IT hardware and software systems are properly maintained, supported, and secure. IT is also responsible for managing the County's IT network, the County's internet and wi-fi connections, database administration, telecommunication systems, cybersecurity, and in-house software development.

The purpose of the audit was to identify and perform tests of internal controls and other IT business operations to determine if:

- Service contract revenue received from the UPD and the Wasatch Front Waste and Recycling District are billed, collected, and accounted for accurately, and comply with the terms of the interlocal agreements.
- IT has implemented adequate authorization and review processes for expenditures and purchases to ensure that expenditures are properly authorized and recorded accurately.
- IT manages County assets in compliance with County policies and if County assets are properly safeguarded against the risk of theft, loss, or misuse.

What We Found

IT did not have a centralized receiving function to ensure that items purchased were received and assigned to the correct employee for accountability purposes.

Based on purchasing records and documents obtained during the audit, we estimated that IT had purchased approximately $803,000 of small-cost items such as office equipment and furniture, desktop computers, laptop computers, hardware, software, peripheral devices, and electronic storage devices, in 2018. We found that IT lacked a formal process for receiving items that employees had purchased and verifying that the correct items and quantities were received.

Establishing proper segregation of duties in the purchasing and receiving processes helps to safeguard County assets against theft, loss, waste, and misuse. With the IT Division's current process, the employee that initiated, and in some cases authorized, the purchase of the items was also the same person who received those items when those items were delivered to the office.

IT had not conducted an annual controlled asset inventory for at least 10 years, making it difficult for them to accurately account for most of those items purchased during that time.

We determined that the IT Division did not have adequate controls in place to ensure that County assets are properly safeguarded against the risk of theft, loss, waste, or abuse. IT assets are highly susceptible to theft and misuse, which adds to the critical nature of these risks and findings. We found that IT was not in compliance with most of the County policies for properly safeguarding County property and assets. IT management should take necessary corrective actions as soon as possible to address these significant risks and findings.

What We Recommend

We recommend that IT involve members of the IT Finance and Administration team in the receiving process to provide adequate segregation of duties and to help ensure that items purchased and received are truly for IT business purposes and that the quantity, cost, and condition of items received match purchase orders.

We recommend that the IT Property Manager develop internal policies for effectively managing the IT Division's controlled assets. The policies should include creating and maintaining current controlled asset inventory lists and standard processes to ensure that proper segregation of duties are in place.

Maintaining a current and accurate controlled asset inventory list is an internal control intended to properly identify and account for county assets that are susceptible to theft or conversion to personal use. The *Controlled Assets Inventory Form – Employee* and the *Controlled Assets Inventory Form – Organization* provides a basis to effectively manage controlled assets. In addition, performing periodic inventories of those assets is an essential process to ensure that all controlled assets in IT are physically present, and properly safeguarded against loss, theft, waste, or abuse.

Summary of Agency Response

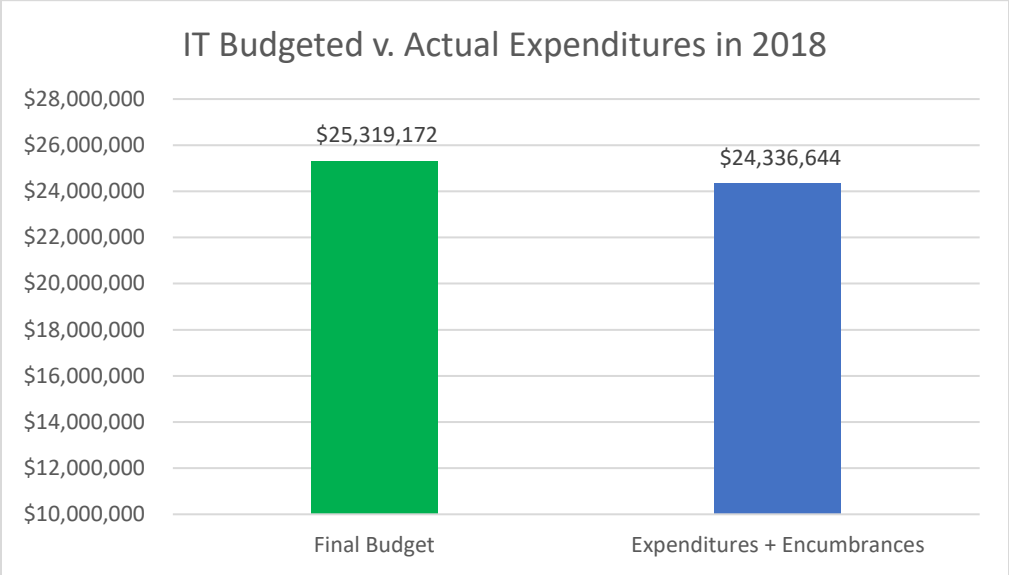
We received a response to the audit from the IT Division regarding the recommendations for improvement given in the report. The response is included at the end of this report. The IT Division has outlined steps and action plans for how they intend to address the issues identified during the audit, and target dates for implementation. A first follow-up audit will be conducted six months from the date of this report, and a final follow-up audit will be conducted in 12 months, to assess the status of implementation of the IT Division's action plans and remediation steps outlined in their response.

Background

The Salt Lake County ("County") Information Technology Division ("IT") provides a broad range of information technology related services for all County offices, departments, and divisions. As an integral part of County operations, IT is responsible for ensuring that the County's IT hardware and software systems are properly maintained, supported, and secure. IT is also responsible for managing the County's IT network, the County's internet and wi-fi connections, database administration, telecommunication systems, cybersecurity, and in-house software development. IT consists of five subdivisions, which include Finance and Administration, IT Infrastructure, Information Security, Applications, and Portfolio Management.

IT is part of the County's Administrative Services Department and its revenue and expenditures are accounted for in the County's General Fund and the Telecommunications portion of the Facilities Services Fund. In 2018, the IT Division's budgeted expenditures were $25,319,172, which also included capital expenditures. The Division's actual expenditures plus encumbrances in 2018 were $24,336,644.

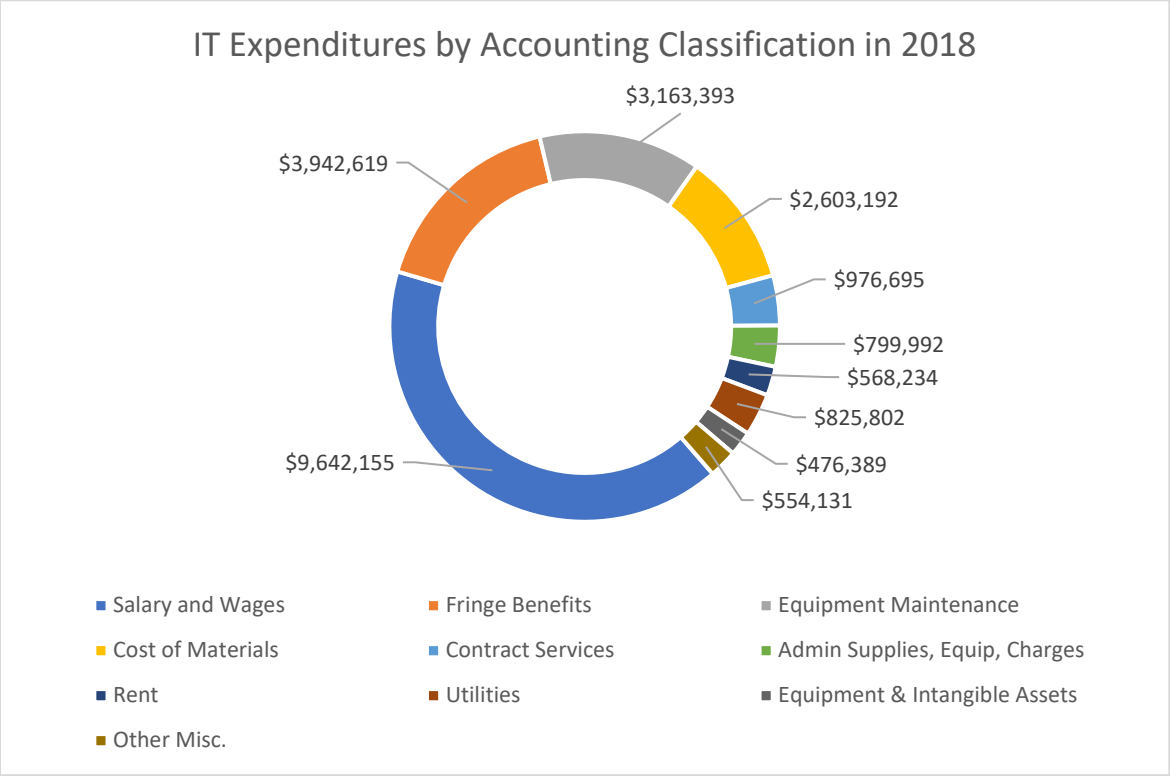
Figure 1. IT Budgeted v. Actual Expenditures in 2018. *The IT Division's total budgeted expenditures for 2018 were $25,319,172. Actual expenditures plus encumbrances were less than budgeted expenditures by approximately $982,528, in 2018.*



Source: PageCenterX – Agency Summary of Obligations vs. Budget Report for FY2018 – IT Division.

The largest expenditure category for IT in 2018 was employee compensation and benefits. IT spent a total of $13.6 million in employee salary and benefits in 2018. They also maintain the majority of the County's IT infrastructure. IT spent $3.2 million for equipment and software maintenance costs in 2018.

Figure 2. IT Expenditures by Accounting Classification 2018. *Employee compensation and benefits made up 58% of total IT expenditures in 2018. After employee compensation and benefits, equipment maintenance costs were the second highest expenditure at 13% of total actual expenditures for the year.*



Source: County Financial System – Actual Expenditures by Organization Report for FY2018 – IT Division.

IT tracks the cost of services provided to each County entity monthly, and then allocates those costs through the County's financial system as indirect costs to those agencies. For example, costs incurred by IT for maintaining and supporting the County's mainframe property tax system are calculated and then charged as indirect costs to the various County property tax offices that are part of the County's Tax Administration Fund.

Occasionally, direct costs such as software licenses or pieces of IT hardware that are purchased by IT on behalf of another County entity are charged directly to the other agency by making accounting entries in the County's financial system. IT also receives service contract revenue for providing a full range of IT related services to the Unified Police Department ("UPD") and the Wasatch Front Waste and Recycling District ("Wasatch") through interlocal agreements. Since these entities are independent of the County, the IT Finance and Administration team manages the contracts with the UPD and Wasatch and bills them directly for those services according to the terms of the agreements.

Objectives

The audit objectives were to identify and perform tests of internal controls and other IT business operations to determine if:

- Service contract revenue received from the UPD and the Wasatch Front Waste and Recycling District are billed, collected, and accounted for accurately, and comply with the terms of the interlocal agreements.
- IT has implemented adequate authorization and review processes for expenditures and purchases to ensure that expenditures are properly authorized and recorded accurately.
- IT manages County assets in compliance with County policies and if County assets are properly safeguarded against the risk of theft, loss, or misuse.

Scope and Methodology

The scope of the audit covered the period from January 1, 2018 through December 31, 2018. The timeline may have been adjusted in some areas when necessary to accomplish the audit objectives. Based upon a risk assessment of IT's business activities and fiscal procedures, our audit work was narrowed to the following areas:

- Service Contract Revenue
- Purchasing and Expenditures
- Capital and Controlled Assets

To accomplish the audit objectives:

- We examined the IT Division's service contracts, monthly billing statements, invoices, and payments made by both the UPD and Wasatch to determine if they complied with contract terms and County policies.
- We reviewed purchasing documents such as purchase orders, invoices, receipts, and packing slips. We observed the IT Division's purchasing and receiving procedures to ensure that IT had implemented adequate segregation of duties, and if they complied with County policies.
- We examined the IT Division's management of County property and assets to provide assurance that they are properly safeguarded against theft, loss, waste, or misuse. We reviewed asset records and documents to determine if IT complied with Countywide Policy 1125, Safeguarding Property/Assets.

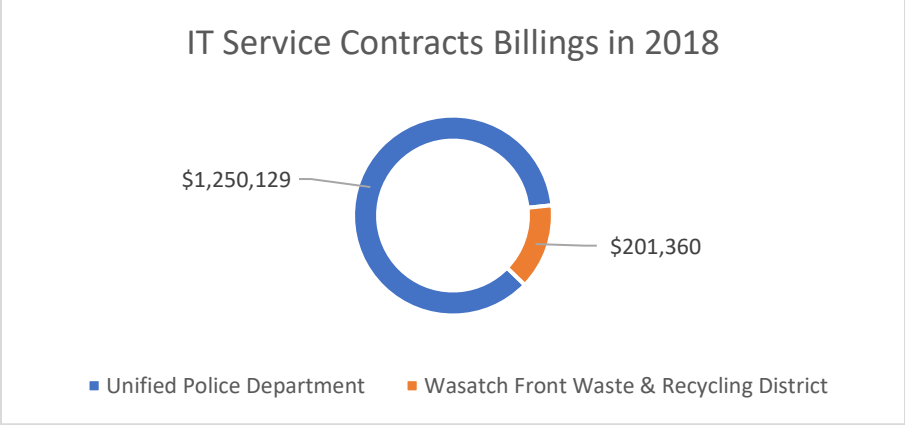
Audit Results

Service Contract Revenue

IT currently has service contracts to provide IT and telecom services to two entities that are not part of Salt Lake County, the Unified Police Department ("UPD") and the Wasatch Front Waste and Recycling District ("Wasatch"). At the end of each month, IT Finance and Administration prepares a billing statement which details the different services each customer received during the month. The IT Accountant creates an invoice and sends a copy of the invoice and billing statement for each customer to review.

Both UPD and Wasatch remit payment to the Mayor's Office of Financial Administration ("Mayor's Financial Administration") by either electronic fund transfer ("EFT") or check. Mayor's Financial Administration then applies the payment to the customer's account in the County's financial system.

Figure 3. IT Service Contracts Billings in 2018. *IT billed a total of $1,451,489 to customers during 2018. The Unified Police Department was billed for over 86% of the IT Division's contract services.*



Source: County Financial System – Service Contract Revenue Report for FY2018 – IT Division.

We examined the IT Division's service contract provisions, monthly billing statements, invoices, and payments made by both UPD and Wasatch to determine if they complied with contract terms and County policies.

Overall, we found that the billing and remittance processes for IT contract services provided to both the UPD and Wasatch did comply with the terms of the contracts and County policies. However, we observed that due dates on billing invoices sent to the IT Division's customers did not always match the terms stated in the service contracts. Specifically, several billing invoices stated that payment was due within 30 days of the invoice, while the contract terms state that payment is due within 20 days of any invoice. While we agree that this is issue is minor, due dates that are not consistent with the terms of the service contracts could cause confusion for customers and make it difficult for IT to enforce the collection of interest on any invoices that are past due.

Findings and Recommendations

Finding 1 – Billing statement due dates were not always consistent with contract terms which led to IT receiving customer payments after the due dates specified in the service contracts.

We examined payments made by UPD and Wasatch from January to December 2018 for contract services that IT provided them. We compared the dates the payments were received to invoice due dates to determine if payments were received on time, and if those payments complied with the terms of the service contracts.

We found that the due dates on most billing statements (or invoices) that IT had sent to both the UPD and Wasatch did not match due dates as stated in the terms of the service contracts. As a result, in 2018, there were a total of nine payments that were received after the due date and grace period as specified in the service contracts. We also noted that these past due invoices should have been assessed an interest charge according to the terms stated in the service contracts but were not.

IT contract with the Unified Police Department states:

> *"The UPD shall remit payment within twenty (20) days of the date of the bill [invoice]... If any said payment is not remitted when due, the County shall be entitled to recover interest thereon. Said interest shall be at the rate of one percent (1 %) per calendar month and shall begin to accrue on the date the remittance is due and payable."*

IT contract with the Wasatch Front Waste and Recycling District states:

> *"The District shall remit payment within twenty (20) days after the date of receipt of the bill [invoice]... If any required payment is not remitted to the County as and when due, the County shall be entitled to recover interest thereon at the rate of one percent (1 %) per calendar month, to accrue from and after the date the remittance is due and payable."*

Instead of the payment due date of 20 days of the date of the bill (or invoice) as stated in the contracts, we found that the billing statements sent to both the UPD and Wasatch indicated that payments were due within 30 days. In 2018, there were nine instances where contract services payments were remitted to IT based on the erroneous due dates stated on the billing statements. We noted that some of the payments were received seven or more days after the two-day grace period allowed by County policy.

Table 1. Payments Received After Contract Due Dates in 2018. *Because of discrepancies between the service contracts and invoice due dates, a total of nine payments for contract services were received after the due date stated in the contracts. We estimated the late payment interest charges based on the terms of the service contracts.*

Payments Received After Contract Due Dates in 2018					
Invoice Date	**Due Date Per Contract**	**Payment Received**	**Days Past Due**	**Outstanding Balance**	**Estimated Interest**
1/31/2018	2/20/2018	3/2/2018	8	$76,959	$202
2/28/2018	3/20/2018	3/29/2018	7	$75,294	$173
3/31/2018	4/20/2018	4/23/2018	1	$72,494	$24
4/30/2018	5/21/2018	5/24/2018	1	$74,105	$24
8/31/2018	9/20/2018	9/26/2018	4	$79,599	$105
9/30/2018	10/22/2018	11/6/2018	13	$80,675	$345
10/31/2018	11/20/2018	11/28/2018	6	$79,312	$156
6/6/2018	6/26/2018	7/2/2018	4	$13,332	$18
7/6/2018	7/26/2018	9/17/2018	51	$15,038	$252
Total Estimated Interest (Not Charged)					**$1,299**

Countywide Policy 1220, Management of Accounts Receivable and Bad Debt Collection, Section 4.4, states:

> *"Payments received after the due date shall be allowed a two-day grace period, following which interest will be charged at 1½ percent per month (18 percent per annum) on the unpaid balance of the account. The interest charged shall be assessed until the account is deemed uncollectible, or until it is referred to the District Attorney's Office."*

To avoid confusion and ensure consistency with the terms of the service contracts, we recommend that that IT revise the payment due dates on the invoices sent to the UPD and Wasatch to reflect the payment terms (within 20 days) as stated in the service contract agreements. IT should also charge interest on any late payments received after the grace period, as stated in the contracts.

Recommendation

We recommend that the IT Fiscal Manager ensure that the due dates on customer invoices match the contract terms and assess interest charges on any past due account balances according to the agreements and County policy.

Purchasing and Expenditures

Overall, we found that the IT Division's internal controls were effective to ensure that purchases and expenditures were properly authorized and recorded accurately and completely. We observed that mistakes had been made in classifying some purchases to the correct accounting codes in the County's financial system. We also noted that the secondary review process that IT had put in place had missed these mistakes as well. We also found that IT lacked a centralized receiving process to ensure that items purchased are received and assigned to the correct employee for accountability purposes. Implementing a centralized receiving process for purchases will help establish better segregation of duties for the purchasing and receiving functions.

Findings and Recommendations

Finding 2 – The IT Contracts Manager made purchases online using another employee's County-issued purchasing card.

We interviewed the IT Contracts Manager to determine if purchases are properly authorized and if all purchases made with County-issued purchasing cards ("p-cards") comply with County policies. During the interview, we were informed that a cardholder's purchasing card information was kept on-file in an online account that both the Contracts Manager and the purchasing cardholder had access to.

The IT Contracts Manager stated that some purchases had been made through the online account using the other employee's p-card, usually when the employee was out of the office. We also discovered that the IT Contracts Manager was responsible for reviewing all purchases made on the other employee's purchasing card, effectively circumventing the segregation of duties that IT management had put in place to prevent fraudulent purchases.

P-card training provided by the Salt Lake County Contracts and Procurement Division (Contracts and Procurement) states that employees are solely responsible for the security of the p-cards issued to them for their use. Section 3.0 of the training manual states:

> *"You are responsible for the security of your card and the transactions made with the card. The card is issued in your name and it will be assumed that any purchases made with the card will have been made by you."*

When we notified IT management of the situation, they acknowledged that it was not acceptable for any employee's purchasing card information to be stored on an online account that another employee had access to. We verified that IT had taken action to remove the employee's purchasing card information from the account.

Recommendation

We recommend that the purchasing card information stored with the online account be deleted, to ensure that cardholders are held responsible for their own purchases and to prevent someone other than the cardholder from making an unauthorized purchase.

Action Taken

We verified that IT management had removed the employee's purchasing card information stored in the online account.

Finding 3 – IT did not have a centralized receiving function to ensure that items purchased were received and assigned to the correct employee for accountability purposes.

Based on purchasing records and documents obtained during the audit, we estimated that IT had purchased approximately $803,000 of small-cost items in 2018. These included items such as office equipment and furniture, desktop computers, laptop computers, hardware and software, peripheral devices, electronic storage devices, etc. In our review of internal controls over the purchasing process, we found that IT lacked a formal process for receiving items that employees had purchased and verifying that the correct items and quantities were received. Shipments of purchased items are generally received at the IT front desk and either taken to the Contracts Manager or directly to the employee or supervisor associated with the purchase.

We selected a sample of 48 purchases (totaling $35,721) that were made in 2018 to review. We examined purchasing records and documentation including purchase orders, packing slips, receipts, and invoices to determine if IT had documented who received the items and if they had verified a count of the items received. We found that in all but two of the purchases in the sample, there was no evidence of who received the items when they arrived, whether the items were for legitimate IT business purposes, or if the quantity of items received was verified against purchase orders or other purchasing records.

Countywide Policy 1125, Safeguarding Property/Assets, Section 2.2 states:

> *"Coordinate with the organization's Purchasing Clerk to ensure all newly acquired property is identified and accountability is appropriately established… [the agency] should ensure proper receiving controls are in place so that property received is what was ordered, and that upon receipt all other property controls explained in the policy are followed."*

Establishing proper segregation of duties in the purchasing and receiving processes helps to safeguard County assets against theft, loss, waste, and misuse. With the IT Division's current process, the employee that initiated, and in some cases authorized, the purchase of the items was also the same person who received those items when those items were delivered to the office. We recommend that IT involve members of the IT Finance and Administration team in the receiving process to provide adequate segregation of duties and to help ensure that items purchased and received are truly for IT business purposes and that the quantity, cost, and condition of items received match purchase orders.

Recommendation

We recommend that IT implement a centralized receiving process for receiving items that are purchased, including requiring a person other than the person who authorized the purchase to verify and document the quantity and condition of the items received.

Action Taken

When we discussed this issue with IT management during the audit, they agreed with the recommendation and had taken some corrective actions to help improve the segregation of duties in their purchasing and receiving procedures. Specifically, IT stated that they had made these changes to their purchasing and receiving procedures prior to the release of this audit report:

- All purchases will be required to go through the point of business (POB) purchasing module which will contain the name of the person who placed the order and the person who has custody of the purchase.
- These will be reviewed by the fiscal manager as part of the purchasing process. All packages delivered to IT will now require a signature from the receiving employee or front desk employee.

Capital and Controlled Assets

Our audit included an examination of the IT Division's management of County property and assets to provide assurance that those assets are properly safeguarded against theft, loss, waste, or misuse. Countywide Policy 1125, Safeguarding Property/Assets, establishes the policies and procedures for the proper management of County capital (fixed) and controlled assets, including procedures for accounting for, protecting, and disposing of those assets.

Mayor's Financial Administration's Accounting Procedures Manual, Chapter 4, Policies & Procedures Relating to Capital Assets, is an additional set of policies and procedures specifically relating to the management of County capital assets. The manual states that some items of personal property are best accounted for and more efficiently maintained by one organization.

Per the Accounting Procedures Manual, Section 4.1.4, IT is:

> *"Responsible for the purchase of network and communication equipment in use throughout the County. Such equipment shall be accounted for on the capital asset accounting records as the responsibility of Information Services."*

We obtained the most recent annual Memorandum of Capital Assets submitted to Mayor's Finance and verified by the IT Associate Director of Finance & Administration on October 17, 2018. The Memo identified the current Property Manager and 536 capital assets listed on the report costing over $16.8 million from the County's PeopleSoft accounting system.

We noted that the capital assets were not only located throughout the County, but also in off-site facilities outside of Salt Lake County. From the 536 capital assets in the IT Division's custody, we selected a sample of 95 to verify the identity and location. The sample included all capital assets costing $100,000 or greater (18 total) and a random selection of 77 additional assets. We were able to verify all 95 capital assets by several methods including physical observation, photographs, and the Cisco Unified Computing System (UCS) admin console.

Table 2. Tools Used by IT to Manage County IT assets. *IT identified the list of tools and how they use these tools to help manage and track County IT assets.*

Tools Used by IT to Manage County IT Assets	
LAN Sweeper	Runs ad hoc searches on the network producing lists of devices connected at the time it is run. This can also provide the model and serial number of most devices.
Big Fix	Runs ad hoc searches on the network producing lists of software running on devices that are actively connected. We are in the process of replacing this with Tanium.
Cisco Prime Infrastructure	A tool that IT uses to manage the network and the equipment. IT can generate inventory reports that tell them where the equipment is located along with the model and serial numbers among other things.
Smart Net Total Care	A product that collects information on all the network equipment and checks that against Cisco maintenance contracts. It provides a report that is like the Prime Infrastructure report but adds information (e.g., if the device is on maintenance, End of Life, etc. and when the device was shipped to IT).
POB	This tool is very manual for us right now. We hope to do some automation of importing data from the collectors that we have into POB. We are also using POB to track purchases of network equipment.
SharePoint	This tool is being used by the IT Security team to track firewalls currently in use on the network.
Excel Spreadsheets	Several of our Associate Directors keep their own spreadsheet lists of software and equipment they maintain. Our Contracts Manager also maintains a master spreadsheet of contracts that includes any contractual agreements for maintenance of equipment and software.

Source: Salt Lake County IT Division.

Countywide Policy 1125, Safeguarding Property/Assets, defines a controlled asset as an item of personal property having a cost of $100 or greater, but less than the current capitalization rate. Due to their nature, controlled assets are more susceptible to theft, or conversion to personal than capital assets. Therefore, controlled assets require additional safeguards against theft or misuse. IT management identified the following tools and how they are being used to help them manage IT assets:

We identified purchases made by IT under the $5,000 asset capitalization threshold in their expenditures line-item categories of computer software, computers and components, and small non-computer equipment made during the four-year period from 2015 to 2018 as recorded in the County's financial system. Total expenditures in those line-item categories for IT were approximately $1.7 million (see Table 3). We determined by reviewing purchasing documents, invoices, and receipts, that most of the expenditures in these categories would meet the criteria for being classified as a controlled asset as defined in Countywide Policy 1125. Therefore, we were able to determine an approximate total cost of controlled asset items purchased by IT each year from 2015 to 2018.

Table 3. Approximate Total Cost of IT Controlled Assets 2015 – 2018. *Purchases made from 2015 to 2018 indicate that IT spent approximately $1.7 million on controlled assets during those years. However, IT did not have a current controlled asset inventory list to be able to positively identify or locate the items purchased.*

Approximate Total Cost of IT Controlled Assets 2015 – 2018					
Asset Type	2015	2016	2017	2018	Total
Computer Software	$70,780	$123,494	($2,056)	$103,932	$296,150
Computers and Components	143,843	152,631	166,604	128,306	591,384
Small Equipment (Non-Computer)	103,825	240,854	382,542	63,802	791,023
Total	**$318,448**	**$516,979**	**$547,090**	**$296,040**	**$1,678,557**

Source: County Financial System – Selected Line-item Expenditures – IT Division Budgets FY2015 to FY2018.

Based on the results of the audit, we determined that the IT Division did not have adequate controls in place to ensure that County assets are properly safeguarded against the risk of theft, loss, waste, or abuse. We identified significant risks and findings in this area. IT assets are highly susceptible to theft and misuse, which adds to the critical nature of these risks and findings. We found that IT was not in compliance with most of the County policies for properly safeguarding County property and assets. IT management should take necessary corrective actions as soon as possible to address these significant risks and findings.

Findings and Recommendations

Finding 4 – IT had not conducted an annual controlled asset inventory for at least 10 years, making it difficult for them to accurately account for most of those items purchased during that time.

In a prior audit conducted by the Salt Lake County Auditor's Office in 2012, we found the following:

- A controlled asset inventory had not been performed for at least two years.
- Seventeen controlled assets could not be located or accounted for.
- Recently purchased controlled assets had not been included on a controlled asset list.
- Employees did not have the *Controlled Assets Inventory Form – Employee* to establish personal accountability for controlled assets that had been assigned to them.

For this audit, we requested all controlled asset inventory forms, records, and supporting documentation. IT could not provide a current controlled asset inventory list or any evidence that they had conducted an inventory of controlled assets within the organization for at least ten years. Countywide Policy 1125, requires all County organizations to keep current controlled asset records, including an inventory list of all controlled assets and *Controlled Assets Inventory Form - Employee* forms for tracking controlled assets that have been assigned to specific employees for their use.

IT was only able to provide five *Controlled Assets Inventory Form - Employee* forms for an organization of over 100 employees. In addition, the five forms that were provided had not been updated and did not accurately reflect the current controlled assets in use by those five employees.

Countywide Policy 1125, Section 2.2, states:

> *"Property Managers assigned by their Administrators are responsible for…At least annually, conduct physical inventory of…controlled assets, to ensure complete accountability for all property owned by, or assigned to the organization."*

Section 4.3, states:

> *"The Property Manager shall maintain records to manage controlled assets using the following forms (or forms that contain substantially the same information) and procedures…'Controlled Assets Inventory Form -Employee' is used for those assets that due to their nature, are used by and therefore readily assignable to an individual…'Controlled Assets Inventory Form - Organization' is used for property not readily assignable to an individual employee or which is shared by more than one employee."*

Maintaining a current and accurate controlled asset inventory list is an internal control intended to properly identify and account for county assets that are more susceptible to theft or conversion to personal use. The *Controlled Assets Inventory Form – Employee* and *Controlled Assets Inventory Form – Organization* provides a basis to effectively manage controlled assets. In addition, performing periodic inventories of those assets is an essential process to ensure that all controlled assets in IT are physically present, and properly safeguarded against loss, theft, waste, or abuse.

Recommendations

1. We recommend that the Property Manager develop internal policies for effectively managing the IT Division's controlled assets. The policies should include creating and maintaining current controlled asset inventory lists and processes to ensure that proper segregation of duties are in place.
2. We recommend that the Property Manager conduct an annual inventory of all controlled assets under the control of the IT Division, using the *Controlled Assets Inventory Form – Organization* or similar form, as required by Countywide Policy 1125. IT management should certify and finalize the results of the inventory upon completion each year.
3. We recommend that IT management ensure that IT employees complete and sign a *Controlled Assets Inventory Form – Employee*, or similar form, to acknowledge personal accountability for controlled assets that have been assigned to them.

Finding 5 – IT did not have a current controlled asset inventory list or a standardized process to ensure that new controlled assets are added to their controlled asset inventory list in a timely manner when purchased.

We found that IT did not maintain a current inventory list of all controlled assets as required by Countywide Policy 1125. We also found that IT had not implemented a standardized process or procedure to add new controlled assets to the controlled asset inventory list when they are purchased.

Relying on purchasing documents, receipts, and invoices from 2018, we identified over 200 new items purchased during the year that met the criteria of being classified as controlled assets. We estimated

that the original cost of these items purchased in 2018 was at least $82,622. To conduct our audit tests, we selected a sample of 99 of these items to determine if they could be identified and located.

Since IT could not provide a current controlled asset inventory list, trying to positively identify and locate those 99 items took a considerable amount of time and research for IT staff to provide evidence that the assets had not been lost, stolen, or otherwise misused by IT employees.

We were able to identify and locate 97 out of the 99 controlled assets in the sample, either through physical observation or by pictures emailed to us from locations outside the County Government Center. IT staff informed us that the two controlled assets that could not be located had been reported lost or stolen by an IT employee who had the assets with him while outside of the Government Center. However, we were not able to verify that this is what happened to the missing controlled assets, or if the employee was ever held accountable for the missing assets that had been assigned to him.

Countywide Policy 1125, Section 2.2, states:

> *"Property Managers assigned by their Administrators are responsible for the following…Accounting for all controlled assets within the organization's operational and/or physical custody…Maintain records as to current physical location of all ~~fixed~~ [capital] assets and controlled assets within the organization's operational and/or physical custody."*

Creating and maintaining a controlled asset inventory list is an important internal control intended to safeguard County assets against the risk of theft, loss, or misappropriation. County organizations are required to maintain a controlled asset list and conduct a physical inventory of controlled assets at least annually, by Countywide Policy 1125. We recommend that IT create and maintain a detailed list of controlled assets and conduct an inventory of those items at least once a year to ensure proper accountability. Also, we recommend that IT develop a process of adding items to the controlled asset list that meet the criteria of a controlled asset when those items are received.

Recommendations

1. We recommend that the IT Property Manager identify all current controlled assets and create a list with all data components necessary to properly account for them.
2. We recommend that the IT Property Manager develop a process to add all newly acquired controlled assets to the list upon receiving them and assign accountability for them either to individual employees, IT teams, or the organization.
3. We recommend that the IT Property Manager ensure that the controlled asset descriptions and locations on the list are accurate and updated as changes occur.
4. We recommend the IT Property Manager develop a controlled asset identification tagging system to better track and identify all controlled assets in the IT Division's custody.

Finding 6 – IT was not conducting a full inventory of capital assets, even though they had certified that the capital asset list maintained by Mayor's Financial Administration was accurate and complete in 2017 and 2018.

We reviewed the annual capital asset inventories conducted by IT in 2017 and 2018. IT has a substantial list of capital assets in their custody, with over 500 items. We noted that IT had certified that the capital asset lists were accurate and complete to Mayor's Financial Administration in memorandums of "Annual

Capital Asset Inventory," dated December 31, 2017 and October 18, 2018, respectively. We determined that IT had not conducted a full and complete inventory of capital assets or updated critical information about those capital asset records for Mayor's Financial Administration.

Countywide Policy 1125, Section 1.10, defines "Safeguard," as:

> *"Safeguard – to provide internal controls appropriate to the organization's operating environment on a cost-effective basis that adequately protect against the loss of property through theft, misuse, abuse, etc."*

Section 2.2, states:

> *"Property Managers…are responsible for…Safeguard[ing] all property subject to this policy for which the organization has custodial responsibility…At least annually conduct physical inventory of ~~fixed~~ [capital] assets…establish[ing] internal protective controls appropriate for custody of the property assigned."*

Mayor's Financial Administration's Accounting Procedures Manual, Section 4.1.3, states:

> *"At least annually conduct physical inventory of capital assets and controlled assets, to ensure complete accountability for all property owned by, or assigned to, the organization. Property Managers may choose the most convenient time of year to conduct their respective inventory based on their business needs. After each annual inventory is complete, submit form (supplied by the Capital Asset Section) to Mayor's Financial Administration acknowledging accountability for capital assets as listed in MFA_AM_INVENTORY "Capital Asset Inventory by department ID". Inventories are due to MFA no later than December 31 each year.*"

It is important to note that Mayor's Financial Administration is only responsible for maintaining the database of capital assets for accounting and financial reporting purposes. Countywide Policy 1125 requires every County agency to conduct an annual inventory of capital assets to ensure that the database is accurate and complete. This is critical to ensure that the County's financial reports are as accurate as possible.

IT has a substantial inventory of capital assets to account for and verify each year. Some of these assets are located throughout the County and even throughout the State of Utah. The IT Division's Property Manager stated that the large number of IT capital assets and the fact that the assets are not all at a central location, makes conducting the annual capital asset inventory very time consuming and difficult to do with limited resources.

New capital assets are often added, and old capital assets are disposed of before IT can complete the inventory each year. The IT Property Manager also stated that asset information is often missing or incomplete on the capital asset inventory list because some IT capital assets may have been moved or transferred to another agency before the certification date as well.

To help lessen the burden of performing the annual capital asset inventory as of a specific date (December 31st) each year, we recommend that IT develop a process for breaking down the list of capital assets into smaller subsets and conducting the annual inventory of each subset at different times

throughout the year. Each subset of capital assets could be certified as of a certain date during the year, with the last subset being certified for Mayor's Financial Administration before the December 31st deadline. This approach, or a similar process, will help to enable IT to complete the full annual inventory of capital assets each year. Also, this will help improve identification, verification, and accountability for each capital asset that IT is responsible for.

Recommendation

We recommend that the IT Property Manager develop internal capital asset policies and procedures that specify a more efficient and effective method for conducting a complete and accurate inventory of capital assets every year. The policies and procedures should include verifying the accuracy of information on the capital asset list and improve accountability for capital assets under the IT Division's control.

Finding 7 – Missing or inaccurate capital asset details on the IT Division's capital asset inventory list made it difficult to locate and identify specific capital assets for verification purposes.

We found that the IT Division's capital asset inventory list for 2018 was missing key details of certain assets, or that some of the details were inaccurate, making it difficult to verify the existence and location of some of the capital assets we reviewed. As part of the annual capital asset inventory certification process, the IT Property Manager should verify the asset location for each capital asset, and update or change key details and information as needed.

The County's financial system serves as the starting point for all County agencies to conduct an annual inventory of capital assets. As we examined the IT Division's capital asset inventory lists for 2017 and 2018, we noticed that several key pieces of information were either missing or incomplete, making it very difficult to verify or identify the correct capital asset during the audit. The missing or incomplete information included:

- The "as of" date that the capital asset inventory lists were extracted from the County's financial system.
- Identifying a "Salt Lake County Personal Property Transfer/Disposal/Internal Sale Form PM-2," when a capital asset had been transferred to another agency or disposed of.
- The actual date that each capital asset was verified.
- How each capital asset was verified (e.g., physical observation, through photographs, virtually).
- Which IT employee verified each capital asset.
- The physical location of each capital asset.

The IT Division's 2018 annual capital asset inventory list contained 553 capital assets. While there was a column on the list that is intended to be used for the four-digit location code for each capital asset, we found that IT was not consistent in using the column to record the correct location code for several capital assets. This made correctly identifying and locating most of the capital assets we selected for our review very difficult. We also noted that in location code column, IT had recorded written comments such as, "surplus," "storage," or "Confirmed by Phil," in the location code field.

We observed the following from our review of the IT Division's 2018 capital asset inventory:

- Sixty-two (62) capital assets (over 11%) were listed as being located at the State Data Center (SDC) on the certified 2018 capital asset inventory list. However, in the County's financial system, not one of these assets was recorded as being at this location. In fact, a four-digit location code did not exist for this location.
- Eight (8) capital assets were listed as being located at the Richfield Data Center (RDC). None of these assets were recorded as being at that location even though a four-digit location code exists for it.
- Seventy (70) capital assets (over 12%) had written locations on the capital asset inventory list, but the location code field was left blank.

Countywide Policy 1125, Section 2.2, states:

> *"Property Managers…are responsible for…Maintain[ing] records as to current physical location of all ~~fixed~~ [capital] assets and controlled assets within the organization's operational and/or physical custody."*

Mayor's Financial Administration, Accounting Procedure Manual, Section 4.3, Capital Assets Location Code Maintenance, states:

> *"It is the responsibility of the Property Manager to ensure accurate location codes are maintained in PeopleSoft…[A] 4-digit number established by Facilities Management in the PeopleSoft location code table…represents a unique geographical site of facilities either owned by the County, or where capital assets owned by the County are located. The location code in PeopleSoft should be updated on a timely basis by the capital asset team at the direction of the Property Manager whenever the asset is relocated to a different County facility site."*

Maintaining accurate and detailed information about capital assets, including accurate location codes, is an important internal control to ensure that County assets are properly managed and accounted for. When key details of assets are not updated or incomplete, it makes it very difficult to properly locate and identify specific capital assets during the annual capital asset inventory process and increases the likelihood that an asset may be lost, stolen, or misused without being detected by management. We recommend that IT update their capital asset inventory list and ensure that the correct location codes are listed for each capital asset during their next capital asset inventory.

Recommendations

1. We recommend that the IT Property Manager request that Facilities Management establish a location code for the State Data Center and any other locations without location codes in the County's financial system.
2. We recommend that the IT Property Managers report the correct location code for each capital asset to Mayor's Financial Administration when certifying their next annual capital asset inventory.

Agency Response

Agency Response Information Technology Division			
Finding 1 – Billing statement due dates were not always consistent with contract terms which led to IT receiving customer payments after the due dates specified in the service contracts.			
Recommendation(s)	**Agree/ Disagree**	**Action Plan**	**Target Date**
We recommend that the IT Fiscal Manager ensure that the due dates on customer invoices match the contract terms and assess interest charges on any past due account balances according to County policy.	Partially Agree	The IT Division would like to point out that most of the late payments noted by the auditors were less than 10 days past the 20-day deadline and well within the 30 deadlines erroneously printed on the invoices. This is a strong indication that our customers are paying on time and that if the correct deadline had been printed on the invoices, the payments would have been made within the 20-day deadline stated in the contracts. Therefore, the amount of interest lost as calculated by the auditor is misleading. Nevertheless, the IT Division has taken action to correct the due date in the contracts and ensure payments are made on time. The IT Division Fiscal Manager reviews an aging report each month to determine if there are past due invoices that should be assessed interest.	11/1/2020
Finding 2 – The IT Contracts Manager made purchases online using another employee's County-issued purchasing card.			
Recommendation(s)	**Agree/ Disagree**	**Action Plan**	**Target Date**
We recommend that the purchasing card information stored with the online account be deleted, to ensure that cardholders are held responsible for their own purchases and to prevent someone other than the cardholder from making an unauthorized purchase.	Agree	**Action Taken:** We verified the Contracts Manager deleted the p-card information from the online account.	**Implemented**

Finding 3 – IT did not have a centralized receiving function to ensure that items purchased were received and assigned to the correct employee for accountability purposes.

Recommendation(s)	Agree/ Disagree	Action Plan	Target Date
We recommend that IT implement a centralized receiving process for receiving items that are purchased, including requiring a person other than the person who authorized the purchase to verify and document the quantity and condition of the items received.	Agree	As noted by the auditors, we have implemented the POB purchasing module and all purchases are now required to go through the it. The record in POB contains the name of the person who placed the order and the person who has custody of the purchase. These are reviewed by the requester's supervisor, the contracts manager, and the fiscal manager as part of the purchasing process. All packages arriving at the IT Division now require a signature from the receiving employee and are recorded as being received in the POB system after documentation and packing slips have been reviewed by fiscal staff.	06/30/2019

Finding 4 – IT had not conducted an annual controlled asset inventory for at least 10 years, making it difficult for them to accurately account for most of those items purchased during that time.

Recommendation(s)	Agree/ Disagree	Action Plan	Target Date
1. We recommend that the Property Manager develop internal policies for effectively managing the IT Division's controlled assets. The policies should include creating and maintaining current controlled asset inventory lists and processes to ensure that proper segregation of duties are in place.	Agree	The IT Division is in the process of adopting a policy and procedures governing tracking, control, and responsibility for controlled assets. The new policy and procedures will address both recommendations under this finding as follows: Adoption and implementation of this policy is in process and will include individual employee asset lists and a comprehensive division wide controlled asset list.	3/31/2021

2. We recommend that the Property Manager conduct an annual inventory of all controlled assets under the control of the IT Division, using the *Controlled Assets Inventory Form – Organization* or similar form, as required by Countywide Policy 1125. IT management should certify and finalize the results of the inventory upon completion each year.	Agree	The IT Division is in the process of adopting a policy and procedures governing tracking, control, and responsibility for controlled assets. The new policy and procedures will address both recommendations under this finding as follows: Following an initial inventory to establish both the employee lists and the division wide list these lists will be continuously maintained and updated and will be comprehensively reviewed annually with individual accountability assigned using the POB system.	9/30/2021
3. We recommend that IT management ensure that IT employees complete and sign a *Controlled Assets Inventory Form – Employee*, or similar form, to acknowledge personal accountability for controlled assets that have been assigned to them.	Agree	The IT Division is in the process of adopting a policy and procedures governing tracking, control, and responsibility for controlled assets. The new policy and procedures will address both recommendations under this finding as follows: Following an initial inventory to establish both the employee lists and the division wide list these lists will be continuously maintained and updated and will be comprehensively reviewed annually with individual accountability assigned using the POB system.	9/30/2021

Finding 5 – IT did not have a current controlled asset inventory list or a standardized process to ensure that new controlled assets are added to their controlled asset inventory list in a timely manner when purchased.

Recommendation(s)	Agree/ Disagree	Action Plan	Target Date
1. We recommend that the IT Property Manager identify all current controlled assets and create a list with all data components necessary to properly account for them.	Agree	As soon as is practical after the new policy and procedures are adopted by division management, a comprehensive inventory will be completed, and a list created of all controlled assets.	9/30/2021

2. We recommend that the IT Property Manager develop a process to add all newly acquired controlled assets to the list upon receiving them and assign accountability for them either to individual employees, IT teams, or the organization.	Agree	All newly acquired controlled assets are currently being tracked as they are purchased through the POB purchasing module. This data will be used to develop both the comprehensive list of controlled assets and the individual employee lists of assets.	6/30/2019
3. We recommend that the IT Property Manager ensure that the controlled asset descriptions and locations on the list are accurate and updated as changes occur.	Agree	The new policy will require employees to update the locations of controlled assets and those locations will be reviewed at least annually by the Property Manager or delegee.	3/31/2021
4. We recommend the IT Property Manager develop a controlled asset identification tagging system to better track and identify all controlled assets in the IT Division's custody.	Disagree	**Alternative Action Plan:** We have determined that due to staffing issues and the nature of some of our controlled assets a tagging system would not be practical or cost effective at this time. It is our intent to use a combination of serial numbers and model numbers to track controlled assets. **Additional Comments:** Management does not believe the increased risk to the County is substantial and consequently accepts any risks associated with not addressing this audit issue.	3/31/2021

Finding 6 – IT was not conducting a full inventory of capital assets, even though they had certified that the capital asset list maintained by Mayor's Financial Administration was accurate and complete in 2017 and 2018.

Recommendation(s)	Agree/ Disagree	Action Plan	Target Date
We recommend that the IT Property Manager develop internal capital asset policies and procedures that specify a more efficient and effective method for conducting a complete and accurate inventory of capital assets every year. The policies and procedures should include verifying the accuracy of information on the capital asset list and improve accountability for capital assets under the IT Division's control.	Disagree	**Alternative Action Plan:** The IT Division is in the process of adopting a policy and procedures governing tracking, control, and responsibility for capital assets. The new policy and procedures require compliance with all County policies regarding fixed assets. **Additional comments:** The IT Division maintains that the information required by County policy was included in our annual capital asset inventory submission to Mayor's Finance Administration as evidenced by their acceptance of that submission each year. Upon completion of the inventory each year it was reviewed by the Capital Asset Team in Mayor's Finance Administration and any corrections or additions requested by them were made. Therefore, management does not believe there is substantial risk to the County and accepts any risks associated with not addressing this audit issue.	3/3/2021

Finding 7 – Missing or inaccurate capital asset details on the IT Division's capital asset inventory list made it difficult to locate and identify specific capital assets for verification purposes.

Recommendation(s)	Agree/ Disagree	Action Plan	Target Date
1. We recommend that the IT Property Manager request that Facilities Management establish a PeopleSoft location code for the State Data Center and any other locations without location codes in the County's financial system.	Agree	The IT Division has requested that Facilities Management establish location codes for all IT capital asset locations that were previously missing from PeopleSoft.	12/31/2020

2. We recommend that the IT Property Managers report the correct location code for each capital asset to Mayor's Financial Administration when certifying their next annual capital asset inventory.	Partially Agree	The most recent capital asset inventory submission in December 2020 to Mayor's Finance included all current asset location codes from PeopleSoft to the best of our knowledge.	12/31/2020