Audit Report Highlights

Department of IT – Inventory **March 2020**

Total Potential Recoveries[1] = $48,743 **Total Cost Savings[2] = $29,160**

Average Annual DoIT Budget[3] = $27.2 million **County Annual Budget[3] = $1.4**

Why DIA Did This Audit

As part of the 2019 audit plan, DIA selected the Department of Information Technology (DoIT) for an inventory review of assets they hold and oversee. This was due to DoIT's ranking on the Annual Risk Assessment and concerns which materialized during our review of IT contracts during the previous Procurement audit released in 2018. The audit period under review was January 1, 2019 through June 30, 2019. The purpose of this audit was to ensure:

1. Inventory listing is complete and accurate, and
2. Proper safeguards are in place to ensure all IT inventory assets are accounted for through the entire inventory lifecycle – procurement to disposal.

What DIA Found

Internal Audit identified the need for improvement within DoIT related to segregation of duties, internal controls and compliance with Cuyahoga County Administrative Code, Ohio Revised Code, and NIST (cyber security framework).

Some of those important findings are noted below.

- Formal asset policies were not established.
- DoIT uses Cherwell as its asset tracking system of record; it was incomplete and inaccurate.
- Assets awaiting disposal were not securely stored.
- Cherwell and SCCM (tracking software) did not include all trackable asset types.
- Assets were not returned or reassigned during the off-boarding process and data plans were not terminated timely. (See table at right.)

Recommendations have been rated by priority: High, Moderate or Low.
*The report contains **20** recommendations:*

*15 **High** – 30 days to complete*
*1 **Moderate** – 90 days to complete*
*4 **Low** – 180 days to complete*

Data Plans Not Terminated Timely

Time	# of Employees
< 1 year	31
1-2 years	13
2-3 years	16
3-4 years	5
> 4 years	3

[1] *Total amount that could potentially be recovered from overpayments or other revenue sources.*

[2] *The amount the County could potentially save annually by implementing recommendations. Cost savings may not be identified.*

[3] *DoIT's annual budget was taken from the updated 2019 budget approved by Council in December 2018. The County Annual Budget includes operating appropriations from all County funds.*

Audit Report Highlights

Department of IT – Inventory — March 2020

Background

DoIT provides system integration and IT solutions for the county government and other municipalities. DoIT is also responsible for providing technology strategy, network systems, and data and device governance for end-point devices for the County's offices, departments, agencies, boards, and commissions under the jurisdiction of the County Executive. End-point devices are inclusive of mobile devices, laptops, desktops, peripherals and network devices.

What DIA Recommended

During bi-weekly meetings, DIA provided DoIT management with recommendations for improving internal controls. We gave these recommendations during the meetings to lessen potential risks related to the inventory management. Doing so during the course of the fieldwork rather than at the end allows the department a chance to remedy things immediately and have no surprises when the report is written.

DoIT has already implemented many of the recommendations made during the audit. They are working to address the remaining issues noted in this report. Based on their responses, we believe corrective action will be taken to mitigate the risks identified. Management responses follow each recommendation in the report. We made the following recommendations:

- DoIT should develop specific guidelines according to standards and best practices for tracking assets in order to achieve and maintain accurate records, review the policies and procedures annually and revise as necessary.
- DoIT should determine the best method to ensure the completeness and accuracy of asset logging in Cherwell. DoIT should establish a schedule for updating and verifying information, to ensure all fields are complete and accurate.
- DoIT should ensure that all stored assets awaiting disposal be locked inside a secure location and accessible only by authorized IT personnel.
- All assets that store data should be tracked regardless of cost and added to Cherwell. Tracking all IT assets allows DoIT to know what/who is accessing the network and prevents unauthorized users and devices access to the County network.
- DoIT should work with HR to ensure DoIT receives onboarding/ offboarding notifications timely and consistently from all County agencies, both Executive and non-Executive. Optimally, the ERP can be set to update DoIT automatically, streamlining the process.

Internal Audit would like to express our appreciation for the cooperation and assistance received from the Department of IT during this audit. The strides made help improve the County's efficiency and accountability.

Internal Audit Report

Cuyahoga County, Ohio

Department of Internal Audit

IT Inventory
Department of Information Technology
January 1, 2019 – June 30, 2019

Director of Internal Audit: Monica Houston, CPA, CGMA, CFE, CIDA

Audit Manager: Rose Karam, CFE, CIA

Investigative Systems Analyst: John Cornwell

Staff Auditors: Tim Verba, CGFM
Tom Schneider, CPA
Joe Balbier, Esq.
Dawn Meredith

Release Date: 08/05/2020

INTERNAL AUDIT REPORT
Cuyahoga County Department of Information Technology
IT Inventory
Cover Letter

January 2020

To: Deputy Chief Technology Officer Andy Molls, Information Security Officer Jeremy Mio, and Department of Information Technology management

The Department of Internal Audit (DIA) has conducted an inventory audit of the Cuyahoga County Department of Information Technology (referred to in this report as "DoIT") for the period of January 1, 2019 through June 30,2019. The audit objective focused on inventory held and overseen by IT, which includes all Executive locations; IT does not track those held by non-executive agencies except for the Office of Homeless Services. DIA performed audit work ensuring IT inventory is complete and accurate and that there are proper safeguards in place to ensure that all IT inventory assets are accounted for throughout the entire inventory life-cycle (procurement, acquisition, operations/maintenance, and disposal).

To accomplish our objectives DIA conducted interviews with management and staff to review segregation of duties for physical custody of inventory, inventory counts and records, physical access and software tracking. We performed preliminary analytics over inventory counts and a physical inventory on a sample of DoIT assets. In addition, we observed the entire inventory life cycle, reviewed lists and inventory tracking for accuracy and completeness, and evaluated the off-boarding procedures regarding the proper return of DoIT property. DIA identified the need for improvement within DoIT processes related to segregation of duties, internal controls, and compliance with Cuyahoga County Administrative Code (County Code) and Ohio Revised Code (ORC). This report provides the details of our findings.

We conducted this audit in accordance with Generally Accepted Government Auditing Standards and the International Standards for the Professional Practice of Internal Auditing. 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.

Because of the inherent limitations of internal controls, errors or irregularities may occur and not be detected. Also, projection of any current evaluation of the internal control structure to future periods is subject to the risk that procedures may become inadequate due to changes in conditions, or the degree of compliance with the procedures may weaken.

The Department of Internal Audit would like to express our appreciation to the staff of the Department of IT and other departments and agencies that assisted throughout the process for their courtesy and cooperation during this audit. A draft report was provided to the Deputy Chief Technology Officer, Information Security Officer and the current management for comment and their responses are included.

Respectfully,

Monica Houston, CPA, CGMA, CFE, CIDA
Director of Internal Audit

Cc: Cuyahoga County Council
Bill Mason, Chief of Staff
Greg Huth, Law Director
Michael C. O'Malley, Cuyahoga County Prosecutor

Contents

Glossary

IT	Information Technology
NIST	National Institute of Standards and Technology
ORC	Ohio Revised Code
Cherwell	The County's Asset Inventory Management System
Solarwinds	Software scanning tool for network discovery and security
Inventory Life-Cycle	Procurement, receiving, inventorying, assignment/transfers, decommission of assets

Report Details

Purpose

The purpose of this audit was to address concerns about the Department of Information Technology (DoIT) inventory which materialized during the completion of the Office of Procurement and Diversity audit released in 2018.

This audit was performed to assess the adequacy of controls and procedures for procurement, receiving, storage, dispersing, tracking, decommissioning, and disposal of IT assets in DoIT. We conducted our review and evaluation of procedures and controls as deemed necessary, through performing a sample of inventory, document review, compliance research and observing each phase of inventory life cycle.

Audit Objectives

The objectives of this audit were to determine whether:

- DoIT was operating in a control conscious environment with adequate controls in place to effectively and efficiently achieve the organization's goals;
- Proper segregation of duties exists in the entire inventory life cycle;
- DoIT assets were appropriately tracked in inventory and located on County premises;
- DoIT had physical safeguards in place to protect assets from theft, loss, security breaches, or mismanagement.

Scope

The scope of this audit focused on financial and operational controls with the policies, procedures and standards, and compliance with all applicable regulations. This audit covered the DoIT inventory and policy and procedures for the period January 1, 2019 through June 30,2019

Methodology

DIA met with DoIT management and personnel, as well as, performed observations to gain a general understanding of DoIT's inventory tracking and the management and recording of the inventory. We reviewed their policies and procedures. We conducted a walkthrough of our selected sample inventory for accuracy and completeness and tested both list to shelf and shelf to list. We verified the accuracy and completeness of DoIT's inventory tracking methods. DIA observed the physical security of IT assets. Data was combined from various sources to discover any inaccuracies and determine completeness.

DIA's audit of DoIT inventory resulted in the findings detailed in this report. Each finding has recommendation(s) provided to resolve or alleviate the underlying cause that contributed to a finding. Recommendations have been assigned priorities.

Priorities help the department focus on resolving the most concerning issues first. Factors involved in determining the priority of a recommendation include: fiscal impact; the existence, design, and effectiveness of internal controls; compliance with laws, regulations and policies; and effect on the County's reputation or public perception.

High (P1)	The department's **Highest-Ranking Officer's immediate attention** is required on one or more of the criteria below. Corrective action is strongly recommended (30 days).
	Issue has a risk that is high impact to the County's finances, internal controls, compliance with laws, regulations, and policies, effect on the County's reputation or public perception and/or is of high importance to County success/achievement of goals.
Moderate (P2)	The department's **Senior Management's attention** is required on one or more of the criteria below. Corrective action is recommended (90 days).
	Issue has a risk that is medium impact to the County's finances, internal controls, compliance with laws, regulations, and policies, effect on the County's reputation or public perception and/or is of moderate importance to County success/achievement of goals.
Low (P3)	The department's **Management's attention** is required on one or more of the criteria below. Corrective action is recommended (180 days).
	Issue has a risk that is low impact to the County's finances, internal controls, compliance with laws, regulations, and policies, effect on the County's reputation or public perception and/or is of low importance to County success/achievement of goals. The recommendation may improve quality and/or efficacy of processes.

Background

DoIT provides system integration and IT solutions within the county government and other municipalities. DoIT is also responsible for primarily providing technology strategy, network system, data and device governance for end-point devices for the County's offices, departments, agencies, boards, and commissions that are under the jurisdiction of the County Executive. End-point devices are inclusive of mobile devices, laptops, desktops, peripherals and network devices. The overall objective of this audit was to assess whether systems and processes are adequate and appropriate to permit the proper accountability of the end-point devices.

Governance and accountability are generally described as maintaining adequate records that permit the County to:

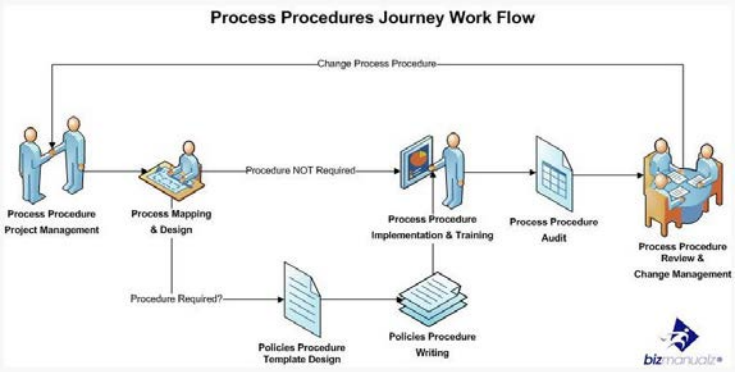
- Know the quantity, quality, location, condition, and value of assets
- Safeguard assets from physical deterioration, theft, loss, or mismanagement
- Minimize unnecessary storage or maintenance costs
- Properly recognize, allocate, or otherwise charge the use/requisition/ depletion of these assets to the proper program/accounting period etc.
- Gather reliable, accurate information to make informed decisions.

Commendable Practices

DIA commends the Department of Information Technology for its cooperation and for implementing many of the suggestions and recommendations DIA made prior to the completion of the audit work. DoIT staff worked with DIA to address its concerns and provide information necessary to evaluate DoIT's inventory processes. DIA further commends DoIT for using this opportunity to improve its internal controls over inventory.

FINDING Formal Asset Control Policies and Procedures Not Established

An asset management plan is the cornerstone for an effective IT asset management (ITAM) system. The plan provides a road map for the organization to understand their objectives and long-term asset management strategy. Written policies and procedures function like a rule book for day-to-day operations to eliminate confusion, create structure, and enforce uniform standards throughout an operation.



An ITAM policy manual should contain the forms and processes that employees will refer to, and is most effective when policies and procedures are clearly documented and reference guides are included. Employees can get up to speed faster and produce consistent results. The policy should reference ORC 305.18 dealing with annual inventory practices and the County's Inventory Policy A202-17.002 which includes IT inventory that meets the valuation threshold: $500 - $9,999 and a useful life longer than 3 years –OR– >$10,000 and a useful life from 1-5 years.

IT assets should not be confused with nor tracked with other organizational assets such as furniture. Maintaining security is one of the main reasons to track IT assets. A special IT asset tracking policy enables the organization to take measures to protect data and networking resources. These policies help prevent the loss of data and organizational assets and reduce risk of a data breach or loss due to poor planning. The average public sector breach costs $2.3 million, but can range from $5 million to $20 million. The Security Officer is ultimately responsible for the development, implementation and enforcement of this policy. And have a

An IT Asset Management (ITAM) Policy and Procedure Manual, is a specific IT asset tracking policy which enables the organization to:

- take measures to protect data and networking resources;
- define what must be done when a piece of property is moved from one location to another;
- help network administrators protect the network by enabling them to know what user and computer is at what station in the event of a network intrusion;
- provide for an up-to-date asset tracking database so that the location of all computer equipment is known at all times; and

- ensure a computer or tablet containing sensitive data being moved between secure facilities is appropriately encrypted while in transit.

It is important that an asset disposal policy be tied to an IT asset usage policy as they involve many of the same issues. This policy impacts many different aspects of the organization and should be developed and coordinated with stakeholders within the Procurement, IT, Risk Management, and Facilities Management departments.

A properly enforced ITAM policy will not only enable organizational assets to be tracked relative to their location and users, but will also ensure the protection of any data being stored on those assets; it will also cover the disposal of IT assets.

DoIT uses Cherwell computer software to track and manage their inventory. Through interviews with the Department of IT (DoIT) personnel and walkthroughs of processes relating to IT inventory management, DIA identified processes that were not fully defined in DoIT's ITAM policies and procedures. As a result, DIA found inconsistencies in the processes followed by DoIT employees for tracking IT assets in Cherwell. These inconsistencies led to inaccurate and unreliable information for DoIT management's use to make informed, business-driven decisions regarding their IT assets. In addition, Cherwell does not track deleted items or leave an audit trail when items are deleted. Although DoIT did have some written policies and procedures, they were neither comprehensive nor enforced.

Risk to the County if Not Corrected

Lack of written internal guidance can result in undefined procedures and inconsistency in the operations, inaccurate reporting records, risk of noncompliance, as well as actions inconsistent with the intentions of management and the County. Without a policy to deal with active and deleted items, the County is at risk of asset misappropriation and poor decision-making based on inaccurate information. In addition, work may not be completed accurately and consistently when vacancies or absences occur.

Recommendations

1. (**P1**) DoIT should develop specific guidelines according to standards and best practices for tracking assets in order to achieve an accurate record. The guidelines below are not meant as an exhaustive list, and policies should be reviewed annually and revised as necessary.

- Specify the parameters to be met by the types of assets to track (type and/or dollar amount threshold), including County guidelines, IT's draft inventory policy and County Inventory Policy A202-17.002. If DoIT decides the County would benefit from tracking other categories of peripheral items (monitors, docking stations, etc.) then all assets that fall within these categories should be tracked;
- The timeframes for updating the entry in Cherwell;
- How assets are tracked, the fields necessary for tracking, and define each of the asset statuses to track the asset throughout its life-cycle (e.g. active, inactive, disposed); and
- The method by which assets in storage are tracked, including stored and not-yet-deployed assets.

Management's Response: ***Throughout the audit, the Department of IT already began drafting a revised policy that addressed the concerns identified by IA. A full draft of the revised policy is completed and is under review by department management. The revised policy will be approved and implemented within 30 days.***

Implementation Date: ***8/5/2020***

2. (**P1**) DoIT should determine the best method to ensure the completeness and accuracy of asset logging in Cherwell. Since DoIT has begun weekly meetings to discuss IT inventory, the DoIT managers should discuss any changes that would affect the asset record in Cherwell and verify it was adjusted properly. DoIT should consider the use of a checklist and Active Directory (AD) to identify changes to assets and reconcile with Cherwell to ensure records are accurate and current.

Management's Response: ***During the audit period a new process was implemented to ensure better tracking of assets. Weekly meetings are being held to discuss IT inventory and note any changes. This will allow for better tracking of IT assets. IT will continue this process regarding updating of asset locations and information relating to asset inventory.***

IT will review implementing additional procedures to reconcile to ensure records are accurate. This will be completed by within 30 days.

Implementation Date***: 8/5/2020***

3. (**P1**) DoIT should create a policy to ensure proper document retention of deleted assets with all relevant asset information being tracked and requiring the administrator's signature. Since the Cherwell database does not retain audit logs for deleted items, the policy should assign one administrator who can delete items and provide assurance that an audit log is maintained for each deleted asset. DoIT should ensure the log:

a. includes the necessary information to distinguish an asset and its complete audit history and lists the reason for deletion, and
b. should be signed by:
    i. the individual responsible for determining the reason for deletion,
    ii. the Cherwell administrator who deletes the asset, and
    iii. be reviewed and approved by a DoIT manager who does not have Cherwell Administrator access to delete assets, prior to the deletion taking place.

Management's Response: ***The Department of Information Technology has implemented a deletion log within Office 365 SharePoint to track deletions within each object within the IT Asset Management System. This deletion log denotes general information about each item deleted, the person who requested the deletion, who authorized the deletion, etc.***

Implementation Date: ***1/27/20***

4. **(P1)** DoIT should include in its asset management policy the process of decommissioning/retiring and disposing of an asset. This policy should detail the disposed-asset record retention and which method of disposal to use (by asset type), the responsible employee/position, and the employee/position responsible for handling the disposal. It is important that all disposals are documented. The new policy should include the documented history of disposed assets and follow A202-17.002. DoIT's policy should address the physical safeguards and security over assets to be disposed to ensure no sensitive information leaves the County. All items should be noted appropriately in Cherwell.

- The IT Asset Management policy should address the proper disposition of IT assets, including a description of which assets require specific physical disposition methods, such as overwriting, degaussing, and physical destruction of assets. This should agree to the data governance policy for assets that store sensitive information such as PII or HIPAA.
- The ITAM policy should address methods for following up on any assets disposed by departments without the proper process.

Management's Response: ***Throughout the audit, the Department of IT already began drafting a revised policy that addressed the concerns identified by IA. A full draft of the revised policy is completed and is under review by department management. The drafted policy includes the current existing disposal policy to provide clear understanding of the County disposal process and safeguards that are and were in place before and during the audit.***

The current disposal policy includes the approved disposal methods that have also been reviewed and approved by the Inspector General's Office in previous years. The

revised inventory policy will include reference and information to the disposal policy. The revised policy will be approved and implemented within 30 days.

Implementation Date: ***8/5/2020***

5. (**P3**) DoIT should evaluate the effectiveness of its current ITAM process by performing a yearly asset inventory, as written in their draft policy. DoIT should ask directors to review their department's inventory and identify any changes, and enter any changes to the inventory in Cherwell. Although not an exhaustive list, the policy should include the following:

- Planning: The timing and communicating what assets are excluded (e.g. monitors), and who is performing the inventory;
- Procedures: How DoIT is taking inventory: scanning barcodes, list to shelf, shelf to list; if a supervisor is recounting all inventory or a sample;
- Reporting: Discrepancies should be re-counted and reported to the proper supervisors/commissions/committees; Cherwell should be updated with the correct information;

Adherence to established inventory procedures and guidelines is necessary to ensure accurate reporting. This plan should follow ORC 305.18 and A202-17.002, addressing Annual inventory and the County inventory policy respectively.

Management's Response: ***Throughout the audit, the Department of IT already began drafting a revised policy that addressed the concerns identified by IA. A full draft of the revised policy is completed and is under review by department management. Additional language has been added to the draft policy to provide clear language for the planning, procedures, and reporting. Additional procedures are also being reviewed during the weekly IT Inventory meetings.***

The revised policy will be approved and implemented within 30 days. Revised procedures will be approved and implemented within 180 days.

Implementation Date*: 12/18/2020*

6. (**P1**) DoIT should create procedures to track missing (lost or stolen) inventory in Cherwell. Guidelines should be established to inform the Technology Advisory Committee of the missing assets in accordance with A202-17.002. In its ITAM policy DoIT should address the valuation method for billing departments (e.g. FMV, book, cost) for missing inventory.

Management's Response: ***Throughout the audit, the Department of IT already began drafting a revised policy that addressed the concerns identified by IA. A full draft of the revised policy is completed and is under review by department management.***

Lost or stolen inventory will now also be tracked in the ITAM along with the required reporting in A202-17.002 (Sheriff Protective Services). The method for tracking

lost/stolen items in the ITAM has implemented and will be specified within the revised policy. **The revised policy will be approved and implemented within 30 days.**

Implementation Date: ***8/5/2020***

7. (**P1**) DoIT should create a policy for assigning inventory to help ensure records accurately reflect asset assignments in Cherwell per A202-17.002 C3f through g.

- DIA recommends DoIT consider removing the "if applicable" in its policy for the requirement to assign computers to the specific employee in the system, as all equipment should be assigned to a specific employee for accountability purposes. If equipment is shared, it should be assigned to the supervisor, or a mitigating control should be implemented.

- DoIT's policy should define a process for tracking assets assigned to non-employees, such as contractors, to ensure the asset is returned at the end of the non-employee's term with the County and the asset is updated in Cherwell.

Management's Response: ***Throughout the audit, the Department of IT already began drafting a revised policy that addressed the concerns identified by IA. A full draft of the revised policy is completed and is under review by department management.***

Shared equipment is already required to be assigned to a supervisor and the revised policy has added language to clarify this process. County contractors (non-employees) will follow the same inventory tracking process as contactor access and County employee inventory; a section has been added to the revised policy to clarify this process. The revised policy will be approved and implemented within 30 days.

Implementation Date: ***8/5/2020***

FINDING Cherwell Was Incomplete and Inaccurate

The Department of IT uses Cherwell software to track inventory. Accurate and complete records in Cherwell are important for knowing asset locations, current inventory, and ascertaining what and when additional assets will need to be ordered. The National Institute of Standards and Technology (NIST) is a cybersecurity framework that provides standards, guidelines and best practices the County follows.

According to NIST Special Publication 1800-5B IT Asset Management:

> "In order for financial services sector institutions to make informed, business-driven decisions regarding their IT assets, they must first know what assets they possess, and their status. This information provides the visibility into license utilization, software support costs, unauthorized devices, vulnerabilities, and compliance."

Furthermore, IT assets are defined as:

> "the assets (end points) on the enterprise network that are owned by the enterprise, such as workstations, switches, servers, users' laptops, virtual machines, and other devices. All enterprise assets are monitored from the start of their lifecycle until disposal by the systems in the Tier 2."

Typical monitoring activities are described:

> "In a typical lifecycle, an asset goes through the enrollment, operation, and end-of-life phases. Enrollment usually involves manual activities performed by IT staff such as assigning and tagging the asset with a serial number and barcode, loading a baseline IT image, assigning the asset to an owner, and, finally, recording the serial number as well as other attributes into a database. The attributes might also include primary location, hardware model, baseline IT image, and owner."

An effective IT Asset Management (ITAM) system can:

> "Tie together physical and virtual assets and provide management with a complete picture of what, where, and how assets are being used. ITAM enhances visibility for security analysts, which leads to better asset utilization and security."

DIA performed testing to determine if DoIT was tracking IT assets effectively using an IT asset management system. DIA noted instances where IT assets were not tracked effectively in either Cherwell or spreadsheets used by DoIT to track assets not in Cherwell. DIA attributes this ineffective tracking to the lack of an overall plan for inventory, contributing to employee inconsistency. To evaluate DoIT's tracking of IT assets we used: 1) analytical procedures, 2) physical inventory, and 3) purchase order testing.

1. Analytical Procedures

DIA analyzed reports from Cherwell as well as the other independent listings, for any inconsistencies, omitted information, or results outside of expectations that could indicate potential issues and indicate the need for further review.

Serial Numbers

DIA noted in our Cherwell review of the total population of 2,282 items, there were 84 assets (or 42 pairs of assets) with duplicate serial numbers and 60 assets missing the serial numbers, although other data was filled in. The exact cause for each of the duplicate serial numbers could not be determined.

Table 1 – Serial Number Issues

Issue	Errors Found	Corrected	Not Corrected	Success Rate
Duplicate SNs	84	50	34	60%
Missing SNs	60	14	46	23%

DoIT should be able to resolve the remaining duplicate and missing serial numbers during its next annual physical inventory of IT assets, as required by County Code A202-17.002: Inventory Policy.

Asset Status

Per NIST standards (which DoIT follows): "In a typical lifecycle, an asset goes through the enrollment, operation, and end-of-life phases. Enrollment usually involves manual activities performed by IT staff such as assigning and tagging the asset with a serial number and barcode, loading a baseline IT image, assigning the asset to an owner, and, finally, recording the serial number as well as other attributes into a database. The attributes might also include primary location, hardware model, baseline IT image, and owner."

Based on DIA's physical inventory, we determined the eight status categories used to track assets during the different stages of the life-cycle were not used consistently or accurately and were not adequate to cover all the phases of the asset life. These inconsistencies resulted from processes not fully defined in DoIT's draft ITAM policies and procedures. Generally, DoIT would delete assets from Cherwell once an item was retired but based on our testing results this process was not consistent.

Table 2 summarizes the current asset status categories used for the 4,791 total assets in Cherwell as of 12/20/2019. Table 3 has the new asset status categories proposed by DoIT. It's easy to see how some current status categories overlap and the naming conventions could cause confusion.

Table 2 – Current Asset Status Categories

Active	In Stock	New	Retired	Planned	Down	Reserve Pool	In Repair

During the audit, DoIT provided Internal Audit with the following list of tentative asset status categories that DoIT would implement once policies were finalized and employees trained on the new process.

Table 3 – Proposed Asset Status Categories

In Stock		Deployed		Disposed	Other*
To Be Deployed	To Be Disposed	Active	Not Active		

* Other (Stolen, with ex-employee, known loss)

DoIT uses RET3, a third-party provider, to securely dispose of IT assets. DIA analyzed RET3 disposal reports to test the status accuracy for retired assets listed in Cherwell. There were 63 disposed items in the RET3 reports that were still listed as other than "Retired"; Cherwell (52), and independent spreadsheets (11).

DoIT has a process to dispose of equipment in accordance with County Code A202-17.002(D) and maintains records in the County's OnBase system. What is not defined is a process to ensure the disposed asset status is updated in Cherwell. Cherwell does not retain audit logs for *deleted* items, nor does DoIT. During the audit, DoIT created a draft manual audit log to track these based on DIA's recommendation.

2. Physical Inventory

End-User Devices: DIA conducted a physical inventory of end-user devices at various County agencies. We selected a sample of each type (desktop, laptop, tablet, and desktop mini) proportionate to its overall population to perform the physical inventory testing. The sample was limited to items assigned to 15 County agencies to ensure a manageable number of locations for the testing. We sampled the items from two perspectives:

1) items listed in Cherwell assigned to the agency (list-to-shelf) existed, and
2) a physical examination of other items at the agency's location (shelf to list) to make sure those devices were included in Cherwell.

In the first test, we verified existence and completeness of assets by comparing our selection from the Cherwell list to the actual asset attributes, to ensure it was listed and was accurate. In the second test, we verified the completeness and accuracy of Cherwell by ensuring randomly selected physical items were included and listed accurately in Cherwell. Some assigned users were inaccurate or missing in Cherwell.

In many departments, assets were reissued to a new employee but still listed in Cherwell under the old employee, or assigned to a different employee in the same department. Many were attributed to lacking a consistent process to track movement within departments or inconsistencies stemming from a lack of formalized inventory policy and procedures.

DoIT Storage Areas: DIA also performed a 100% inventory (shelf to list) of IT's storage areas and noted 139 end-user devices in DoIT storage areas not tracked in Cherwell. Recently purchased items were not being entered in Cherwell until they were tagged, configured, and deployed to an end-user. The remaining unlogged items pre-dated the 2018 inventory implementation of Cherwell and a process was not in place to add inactive devices. These were end-user devices previously assigned to employees that were later collected by DoIT and moved into storage, without a consistent process for tracking them.

Table 4 summarizes our results.

Table 4 – End-User Device Test Results

Inventory Testing	1) Agencies	2) Storage Areas
List-to-Shelf (Existence of asset)	134	0
Shelf-to-List (Completeness of list)	183	269
#1 Inventory Test:	**Total**	**Total**
Tested for Existence/Completeness in Cherwell	317	269
Total Items Located and in Cherwell	253	130
Success Rate	**80%**	**48%**

#2 Cherwell Accuracy Test:	Agencies Total	Storage Total
Tested for Cherwell Accuracy:	253	130
Total Attributes Tested (11 per item)	2,783	1,430
Accurate / Inaccurate Attributes in Cherwell	2,377 / 406	980 / 450
Accuracy Rate	(2,377÷2,783) **85%**	(980÷1,430) **69%**

Overall, the asset type, make, model and serial number were 98-100% accurate for the agencies and storage areas. Fields defining the location (room, assigned user, floor) ranged from 11% to 72% accurate. Yet other fields such as building, department and status ranged from 32% (storage areas) to 87% for the agencies.

Network Devices: DIA inventoried 100% of network devices in IT's storage areas and only 6 of 212 (2.8%) were tracked in Cherwell. These items included switches, servers, firewalls, wireless access points and routers. This network equipment pre-dated DoIT's centralization of the County's IT infrastructure. Previously, IT assets were managed independently by various County agencies and no process was in place to add inactive devices.

DoIT does track active network devices and only the retired network devices acquired after the IT centralization. DoIT uses discovery tools, which identify active network devices to update and reconcile its listings. DIA sat down with DoIT personnel to review SolarWinds and Cisco Prime (network device tracking software) to test DoIT's process of updating and reconciling its listings of active and retired network devices. Based on the results of its reviews, DIA determined the process was in place and operating effectively.

3. Purchase Order Testing

We tested invoices of IT purchases to verify the completeness and accuracy in Cherwell and were unable to locate some packing slips (receipt of goods support) with the supporting documentation. As a result, DIA could not validate that all assets received were tracked properly in Cherwell. For those purchases having

adequate support documentation, some were not in Cherwell. We validated the existence of these items during our inventory of DoIT's storage areas. There is not a consistent process in place to track inventory held in storage before it is tagged, configured and deployed to an end-user, or put into use.

DIA was unable to perform a 3-way match (purchase order, packing slip, invoice) to verify proper receiving and logging of assets due to the absence of packing slips. This matching ensures the item(s) in the quantity ordered were received, and invoices were paid for the correct quantity and amount. There was insufficient support to show that the manager was verifying receipt of goods and the IT Analyst was performing a 3-way match to ensure receipt and proper payment. During the audit, DoIT started uploading all the purchase support documentation (purchase order, packing slip, invoice) to a shared drive to ensure the documentation would be retained and available for review. However, DIA is aware that this would still not ensure the reviews would occur consistently.

DIA also noted that purchase information was not entered in Cherwell for each asset. This resulted in difficulty determining the cost of the asset, whether the asset met the capitalization threshold per County policy, and researching the purchase history of an asset for audit purposes.

Risk to the County if Not Corrected

There is an increased fraud risk or improper risk management due to inaccurate and incomplete reporting, which can lead to a loss of IT assets and increase the potential for loss of sensitive and confidential County data. Not knowing what you have and who has it presents an obvious security risk and can also cause management to lose potential leveraging opportunities when allocating or refreshing assets. This can hinder the ability to budget for future IT equipment needs and potentially purchasing additional assets when unused assets are available.

Without a three-way match, the County could be purchasing items that never make it into the system and increase the risk of asset misappropriation or system intrusion if not updated for security purposes.

Recommendations

1. (P1) DoIT should determine the best method to ensure the completeness and accuracy of asset logging in Cherwell. In their weekly meetings to discuss IT inventory and to ensure management's review is consistent and complete, a checklist of the review procedures should be completed at each meeting.

Management's Response: ***During the audit period a new process was implemented to ensure better tracking of assets. Weekly meetings are being***

held to discuss IT inventory and note any changes. This will allow for better tracking of IT assets. IT will continue this process regarding updating of asset locations and information relating to asset inventory.

IT has implemented an intake process upon delivery to automatically update packaging information to then be loaded into the ITAM. IT then reviews all information within the weekly meetings to ensure accuracy. IT is currently testing various automated technologies to audit and review current inventory to ensure the ITAM system is accurate.

IT will review implementing additional procedures to reconcile to ensure records are accurate through the end of 2020. Initial procedures will be completed within 30 days.

Implementation Date: ***8/5/2020***

2. (P1) DoIT should establish a schedule for updating and verifying information, as well as assigning dedicated personnel to the process. DoIT should ensure that any existing assets with missing or inaccurate information (e.g. serial number, location, assigned department, assigned user) are identified and the fields updated. Duplicate serial numbers should be resolved. If DoIT is unable with certainty to identify the true asset record and resolve the duplicate records, DoIT should add an explanation on the records to prevent confusion. In the absence of a unique constraint or required serial number in Cherwell, a monitoring process should be in place to ensure that duplicated or missing serial numbers are discovered and corrected.

Management's Response: ***During the audit period a new process was implemented to ensure better tracking of assets. Weekly meetings are being held to discuss IT inventory and note any changes. This will allow for better tracking of IT assets. IT will continue this process regarding updating of asset information and duplicate information to ensure accuracy.***

IT will review implementing additional procedures to reconcile to ensure records are accurate. This will be completed by the end of 2020. If IT requires additional staffing as suggested by IA, IT will review with HR and the Executive Office.

Implementation Date: 8/5/20

3. (P1) Upon delivery of IT assets, DoIT should record the receipt in Cherwell, or separately track it temporarily in a spreadsheet/log if the asset information is not available (e.g. still in the box), even if it's to be held in storage. Assets should always be tracked, from time of receipt to disposal.

Management's Response: ***During the audit period a new process was implemented to ensure better tracking of assets. Weekly meetings are being held to discuss IT inventory and note any changes. This will allow for better tracking of IT assets.***

The Department of IT is reviewing the most effective process of tracking inventory throughout the entire lifecycle. Currently IT is tracking all deliveries and packaging slips to a network location. Then required information is loaded into the ITAM system. The ITAM system has been updated to include the Purchase Order Number on newly imported assets.

IT will review implementing additional procedures to reconcile to ensure records are accurate. This will be completed by within 30 days.

Implementation Date: ***8/5/2020***

4. (P1) DoIT should implement a 3-way match (invoice, purchase order, packing slip) for effective internal control and ensure all documents are attached to the purchase documentation. Scanning the packing slip when it's received will give all necessary personnel access to it right away. A completed checklist would help ensure all support is received and checked.

Management's Response: ***Throughout the audit, the Department of IT already began drafting a revised policy that addressed the concerns identified by IA. A full draft of the revised policy is completed and is under review by department management.***

Currently IT is tracking all deliveries and packaging slips to a network location. Then required information is loaded into the ITAM system. The ITAM system has been updated during the audit to include the Purchase Order Number on newly imported assets. The revised policy will be approved and implemented within 30 days.

Implementation Date: ***8/5/2020***

5. (P1) DoIT should track purchase information for each asset in Cherwell in accordance with County inventory policy. DoIT should consider entering purchase order numbers for each asset upon receipt of goods to facilitate determining the cost of assets for the annual inventory.

Management's Response: ***Throughout the audit, the Department of IT already began drafting a revised policy that addressed the concerns identified by IA. A full draft of the revised policy is completed and is under review by department management.***

Currently IT is tracking all deliveries and packaging slips to a network location. Then required information is loaded into the ITAM system. The ITAM system has been updated during the audit to include the Purchase Order Number on newly imported assets. The revised policy will be approved and implemented within 30 days.

Implementation Date: ***8/5/2020***

6. (**P1**) DoIT should consider asking agencies with DoIT-managed IT inventory to track their listings of IT inventory (used, unused/in storage) to ensure that reassigned assets are updated in Cherwell. A supervisor should manage this list to help ensure DoIT's listings are kept complete and up to date.

Management's Response: ***The Department of Information Technology will work with the agency representatives to validate the assets are correct on an annual basis in compliance with the County's inventory process. The revised policy will include this process and be approved and implemented within 30 days.***

Implementation Date: ***8/5/2020***

FINDING Assets to Be Disposed Were Not Stored Securely

The key reason to track IT assets, other than for property control, is to maintain data security. An IT asset tracking policy enables the organization to take measures to protect data and networking resources. These policies help prevent the loss of data or organizational assets and reduce risk of a data breach or loss due to poor planning. The Security Officer is ultimately responsible for the development, implementation and enforcement of this policy.

Care should be taken to ensure that all data contained on the devices has been removed or the device is destroyed and made unreadable. For organizations to have appropriate control of the information they are responsible for safeguarding, they must properly secure and dispose of used media.

DoIT's draft inventory policy does not specify media sanitization methods and a secure location for temporary storage of IT assets designated for disposal. When an IT asset is no longer in use by an agency and DoIT determines it cannot be repurposed, the policy specifies that the equipment must be disposed of. The County has contracted with RET3, a full-service non-profit providing secure disposal of electronic equipment.

During a walkthrough of the disposal process, we observed components stored in a semi-secure location. Although the storage area where the assets were held is only accessible to active County employees with badge access, it is not restricted to DoIT personnel only. Due to limited space, DoIT stored the assets awaiting disposal on pallets outside their caged area.

Furthermore, the caged area was not adequate for securing IT assets, because of its shared access and space with other County agencies storing files. During the audit, DoIT was able to free up storage space by reorganizing and disposing of obsolete assets, but the shared access remained.

Risk to the County if Not Corrected

Confidential information or County data stored on computer hard drives and backups in employee-accessible areas are at risk of being accessed by unauthorized personnel which could result in a data breach, security risks, fines or reputational damage. In addition, the physical hardware itself is subject to asset misappropriation.

Recommendation

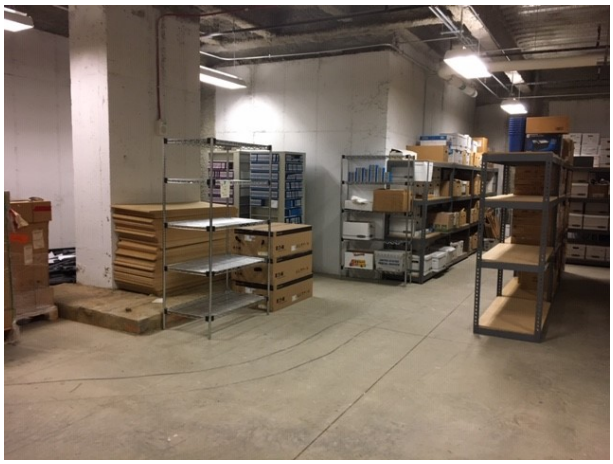
1. (P1) DoIT should ensure that all stored assets awaiting disposal be locked inside a secure location and accessible only by authorized IT personnel, such as the cage area. We recommend cameras be installed in the cage area, especially with the upcoming computer refresh creating an influx of new equipment.

   Update 3/9/20: To address our security concerns, DIA and DoIT worked in cooperation with Public Works and the County's building management company to partition off the cage area, so DoIT could have a dedicated space accessible only to DoIT for securing its assets. The building management company installed a fence to divide the cage where DoIT assets are stored. However, there are still file boxes belonging to other departments inside the IT designated area.

Management's Response: ***The Department of IT has acquired a dedicated secured cage area for IT equipment. Access to the caged area currently has cameras and IT maintains a separate log sheet for cage access.***

The Department of Information Technology will work with the agencies who currently store files within the IT Department's cage to relocate those items elsewhere. Please refer to the pictures below.

Implementation Date:*6/16/2020*



FINDING Cherwell and SCCM Do Not Include All Trackable IT Asset Types

Maintaining a centralized inventory with reliable information of all IT equipment is critical for overall organizational system security, efficiency and effectiveness. Accurate and complete records in Cherwell are important for knowing asset locations, current inventory, and ascertaining what and when additional assets will be needed.

According to NIST, the cybersecurity framework DoIT follows, knowing what assets you possess and their status *"provides the visibility into license utilization, software support costs, unauthorized devices, vulnerabilities, and compliance*." IT assets are defined by NIST as *"the assets (end points) on the network…such as workstations, switches, servers, users' laptops, virtual machines, and other devices. All enterprise assets are monitored from the start of their lifecycle until disposal by the systems in the Tier 2."*

The location of all computer equipment should be known (or knowable) at all times. This helps network administrators protect the network by enabling them to know what user and computer is at what station, in the event of a network intrusion.

General types of assets subject to tracking include:

1. Desktop workstations
2. Laptop mobile computers
3. Mobile phones and tablets
4. Printers, Copiers, Fax machines
5. Handheld devices
6. Scanners
7. Servers
8. Firewalls
9. Routers
10. Switches
11. Memory devices
12. Software

Cherwell's inventory tracking does not include mobile phones, VoIP phones, servers, network equipment, or software. Rather, the Department of IT uses spreadsheets to track all active and decommissioned mobile phones, VoIP phones, servers, and

network equipment. Software is tracked through SolarWinds, an IT network performance monitoring software and remote monitoring tool.

Cherwell's database is neither centralized nor all-inclusive. During our audit, DoIT started the planning process of incorporating other asset types in the Cherwell system.

DoIT does not have a comprehensive listing of software used by the County for inventory purposes. DIA received a report DoIT generated from Microsoft's System Center Configuration Manager (SCCM) which lists most, but not all, software installed on computers accessing the County network. SCCM does not include software used by various agencies that either is not detected by SCCM or resides on a server that is not actively managed by DoIT.

DoIT does not track software and licenses as inventory. From an operational perspective they are not often involved in actively supporting software on behalf of agencies. However, DoIT does have a responsibility from a security compliance perspective, including protecting personally identifiable information, and therefore should track all software and licenses, including manual entries for software outside of what is tracked in SCCM.

Risk to the County if Not Corrected

Non-compliance with NIST and industry best practices stops DoIT from effectively tracking the assets on hand and risks a data breach as a result of outdated inventory. Spreading the inventory information through Cherwell and various spreadsheets makes presenting a complete picture a multi-step process of consolidating all the data in one place. In addition to security issues, poorly informed management decisions regarding software in use can create overlap of assets, possible licensing issues resulting in fines, and inhibit County savings when purchasing in bulk. Manual tracking of assets can result in inconsistencies with inventory management.

Recommendation

1. (**P3**) Assets costing less than $500 which do not contain data should not be specifically tracked. These include components such as video or sound cards. However, all assets that store data should be tracked regardless of cost. IT should add all IT asset types to Cherwell. DoIT includes smartphones as trackable assets because of the ability to access sensitive information. Tracking all IT assets allows DoIT to know what/who is accessing the network and prevents unauthorized users and devices access to the County network.

Management's Response: ***Throughout the audit, the Department of IT already began drafting a revised policy that addressed the concerns identified by IA. A full draft of the revised policy is completed and is under review by department management.***

All assets regardless of cost (<$500) that contain sensitive data will be tracked. Data security and data classification are covered under other IT policies. This revised policy will include language and a process of tracking assets that cost less than $500. The revised policy will be approved and implemented within 30 days. Smartphones are currently tracked separately but till be tracked in the ITAM within 180 days.

Implementation Date: ***12/18/2020***

2. (**P3**) DoIT should develop a plan for migrating its IT assets tracked in the independent listings (mobile devices, VoIP phones, severs, network equipment) to Cherwell. DoIT should determine which fields are necessary for each type of asset and establish the protocol/policy to ensure personnel will track each asset type consistently. DoIT should incorporate all fields necessary to distinguish the asset and establish custody throughout the entire life cycle of the asset.

Management's Response: ***Throughout the audit, the Department of IT already began drafting a revised policy that addressed the concerns identified by IA. A full draft of the revised policy is completed and is under review by department management. The revised policy will be approved and implemented within 30 days.***

IT will then develop a plan within 180 days to update the ITAM (Cherwell) with all IT tracked assets (per the approved policy) to be implemented by the end of 2020.

Implementation Date: ***12/18/2020***

3. (**P3**) Because DoIT has a responsibility to track all software and licenses from a security compliance perspective, DoIT should determine the most effective and practical method for maintaining the listing that will allow for manual entries outside of what is tracked in SCCM.

Management's Response: ***The Department of Information Technology will review the capabilities and resources required to meet IA recommendations. IT will determine the most effective and practical method by end of year 2020.***

Implementation Date: ***12/31/2020***

FINDING Assets Not Returned or Reassigned During Offboarding

When an employee is hired by the County, they are issued IT equipment based on their position and role. When that employee is terminated (resigns, retires, etc.) they are expected to turn in any badges and equipment charged to them. IT is notified by Human Resources (HR) and any IT equipment should be returned to them for re-imaging and possible use by another employee.

During our physical inventory we identified former employees' PCs sitting at empty desks and the former employees still listed as the assigned user in Cherwell. In addition, mobile phone accounts were still active after employees left the County.

As soon as a supervisor is notified an employee will be leaving their department, permanently or temporarily, the supervisor should notify their HR Analyst. HR sends an email to notify DoIT of the change to the employee's status. Attached to the email is a copy of the employee's signed Employee Information Form detailing equipment the employee was previously provided.

On the employee's last day at their work location, DoIT should collect the assigned IT equipment and have the employee sign the Employee Information Form showing that the equipment has been turned in and submit this to HR. Upon issuance of mobile devices, employees sign the County Employee Policy Agreement, including the requirement to "return device(s) upon termination, collected by Supervisor". The policy defines the types of mobile devices that apply:

- Smartphones and other mobile/cellular phones;
- Tablet computers, E-readers, PDAs and other portable media devices;
- Laptop/notebook computers; or
- Any mobile device capable of storing County data and connecting to a network"

During DIA's physical inventory, we noted inconsistencies in the handling of mobile devices upon termination, inaccuracies in the recordkeeping of desktops, laptops, cell phones and tablets in Cherwell. At County agencies we observed desktops and laptops at unoccupied cubicles, in shared storage closets, and the cabinets of employee offices. Although we were able to reconcile some of the devices with a record in Cherwell, the records still listed the terminated employee assigned to the device, and a supervisor was not identified to establish custody.

DoIT lacks a process to re-establish custody and accountability of these devices. We also observed desktops and laptops that were re-assigned to another employee but the record in Cherwell still had the terminated employee assigned to the device.

DIA did not do a physical inventory of wireless telecommunication devices such as cell phones, hotspots, aircards, cameras. Instead, we relied on analytical procedures to determine if the devices were returned, and associated wireless plans deactivated, as part of the off-boarding process. As part of DIA's analytical procedures, we compared the Wireless Plans listing to employee records to ensure the assigned users were active employees.

The Wireless Plans report is generated from the County's online account listing mobile phone voice/data plans with AT&T. We identified 68 active plans assigned to the names of former employees, which DoIT deactivated during the audit. We confirmed with DoIT that the cost of the physical phones was only $1.00, so we did not attempt to locate the physical assets. However, since there was a service cost associated with plans staying active after an employee left, these should have been deactivated during the offboarding process. The cost of these 68 expired plans totaled $48,743. The plans were not being deactivated due to the lack of a review process to ensure all offboarding notifications from HR were received and the necessary steps taken by the administrator over the devices.

Risk to the County if Not Corrected

There is a data security risk for both laptops and phones that are not turned in if the employee continues to have access to the County's network. There is also the risk of theft if a supervisor is not assigned to oversee the asset. Active mobile phone plans remaining after an employee leaves incur unnecessary costs to the County.

Recommendation

1. (**P1**) DoIT should establish an internal policy and the necessary forms to ensure a clear and consistent process for returning device(s) upon termination. These should be collected by a supervisor or reassigned to another employee through DoIT. The internal policy should ensure that custody and accountability of devices is always maintained and that the records in Cherwell or the appropriate inventory listings are updated to reflect the new assignment.

Management's Response: ***Throughout the audit, the Department of IT already began drafting a revised policy that addressed the concerns identified by IA. A full draft of the revised policy is completed and is under review by department management.***
The revised policy has specific procedures defined for Human Resources to notify IT of employee changes, including termination and offboarding. The revised policy will be approved and implemented within 30 days.

Implementation Date: ***8/5/2020***

2. (**P1**) DoIT should work with HR to ensure DoIT receives onboarding/offboarding notifications timely and consistently from all County agencies, both Executive and non-Executive. DoIT should coordinate with HR to have summaries sent to IT at least monthly of all the terminated employees. This would be in addition to the periodic ones currently sent, to ensure that none of the offboarding e-mails were missed or not responded to properly by DoIT. If possible, the ERP should provide automated notifications during the onboarding/offboarding process, so DoIT is able to manage changes to mobile devices timely and consistently.

Management's Response: ***The Department of IT is already receiving ERP information bi-weekly to ensure access is disabled for onboarding and offboarding. The Department of IT has further implemented (starting on 7/1/2020) location information to be integrated from ERP into the IT Directory (Windows Active Directory) system. This information can then be used to dynamically update and alert changes in the ITAM.***

IT has completed implementing all available information to trigger onboarding/ offboarding and location update information. The ERP will also include automatic notification in the scope for the ERP project. This is scheduled to be implemented within the ERP go-live window. Full recommendations require dependent items within ERP. DoIT will be able to complete all recommendations possible within 30 days.

Implementation Date: ***8/5/2020***

3. (**P2**) Management should review the inventory listing, County Employee [Mobile Device] Policy Agreements, and system reports (Wireless Plans and inactivity reports) regularly to ensure accountability over both the devices and the associated wireless plans, and timely termination of plans.

Management's Response: ***The Department of IT conducts monthly reviews of mobile usage and contacts agencies and departments for any devices without any billed activity. The Department of IT will work with department management to make sure devices are properly assigned to ensure the ITAM is updated. This will be completed within 60 days.***

Implementation Date: ***9/4/2020***