Office of Legislative

Auditor General

SEAL OF THE CHARTER COUNTY OF WAYNE, MICHIGAN 1796
WE PRODUCE IN GOD WE TRUST WE DEFEND
FREEDOM OF MAN

MARCELLA CORA CPA, CIA, CICA, CGMA
AUDITOR GENERAL

500 GRISWOLD STREET
STE. 842 GUARDIAN BLDG
DETROIT, MICHIGAN 48226

TELEPHONE: (313) 224-8354

April 25, 2022

FINAL REPORT TRANSMITTAL LETTER

Honorable Wayne County Commission:

Enclosed is our final copy of the Office of Legislative Auditor General's report on the Wayne County Department of Information Technology, Controls Over Computer Assets. Our report is dated April 7, 2022; DAP No. 2020-57-005. The report was accepted by the Committee on Audit at its meeting held on April 13, 2022 and formally received by the Wayne County Commission on April 21, 2022.

We are pleased to inform you that officials from the Department of Information Technology provided their full cooperation. If you have any questions, concerns, or desire to discuss the report in greater detail, we would be happy to do so at your convenience. This report is intended for your information and should not be used for any other purpose. Copies of all Office of Legislative Auditor General's reports can be found on our website at: https://www.waynecounty.com/elected/commission/oag/legislative-auditor.aspx.

Sincerely,

Marcella Cora

Marcella Cora, CPA, CIA, CGMA, CICA
Auditor General

REPORT DISTRIBUTION

Wayne County Department of Technology
Hector Roman, Director
Ryan Hayes, Director, Enterprise Computing & Infrastructure

Wayne County Department of Management & Budget
Hughey Newsome, Chief Financial Officer
Yogesh Gusani, Deputy Chief Financial Officer
Shauntika Bullard, Director, Grants, Compliance and Contract Management

Wayne County Executive

County of Wayne, Michigan

Department of Information Technology (DoIT)

CONTROLS OVER COMPUTER ASSETS

Performance Audit
April 7, 2022

DAP No. 2020-57-005

EXECUTIVE SUMMARY

Type of Engagement, Scope, and Audit Methodology

The Office of Legislative Auditor General conducted a performance audit of the Department of Information Technology (DoIT), Controls Over Computer Assets. This type of engagement provides an objective analysis to assist management and those charged with governance and oversight. The information contained in this audit report is intended to assist key stakeholders in the improvement of controls within the County.

Our initial engagement scope and objective was to assess DoIT controls over the accountability of inventory, authorized assignment, and disposal of computer assets for the period of October 1, 2018 through June 30, 2020. However, we were subsequently informed that the department had purchased one-thousand laptop computers with CARES (Coronavirus Aid, Relief, and Economic Security) Act grant funding received during fiscal year 2020. Therefore, we modified our engagement scope to also include the remainder of fiscal year 2020 and 2021 to assess the CARES Act laptop computer purchases.

Our engagement was primarily conducted remotely due to the safety protocols established by State and local officials in response to the COVID-19 pandemic. We conducted discussions and walkthroughs with DoIT management to understand the computer inventory management process. We also conducted limited on-site observations at the Guardian Building and examined the electronic records stored on the department’s SharePoint site.

Introduction

The Department of Information Technology (DoIT) is required to maintain accountability over all computer assets that are purchased and held by the County. In fiscal year 2018, DoIT purchased the Ivanti Service Management platform, to better manage incoming service desk tickets, and to help improve the department’s computer asset management capabilities, change management functionality, and reporting abilities.

As noted in the county budget appropriations, DoIT is appropriated $1.2 Million of funding each year to replace older computers through the Tech Refresh Program. Under this program, standard desktop computers are to be replaced every five (5) years, and standard laptop computers are to be replaced every three (3) years to comply to IT industry standards. DoIT also received roughly $1.04 Million of CARES Act grant funds during fiscal year 2020 to purchase laptop computers for County employees.

SUMMARY OF ISSUES

AUDIT OBJECTIVE #1:

ASSESS DOIT CONTROLS OVER THE ACCOUNTABILITY OVER INVENTORY, AUTHORIZED ASSIGNMENT, AND DISPOSAL OF COMPUTER ASSET.

Issue Identified	Type of Issue
2020-01 Enhance Policies for DoIT Operational Procedures (Pg. 7)	Control Deficiency
2020-02 Establish Written Agreement with Disposal Vendor (Pg. 8)	Control Deficiency
2020-03 Improve Record of Hard Drive Sanitization (Pg. 9).	Control Deficiency
2020-04 Conduct Periodic Inventory Checks (Pg. 11)	Control Deficiency
2020-05 Strengthen Controls Over the Management of Computer Inventory (Pg. 13)	Control Deficiency
2020-06 Enhance Documentation Over the Receiving and Distribution Process (Pg. 15)	Control Deficiency

Views of Responsible Officials

We shared the results of our audit with DoIT management, and discussed the issues noted above, and have incorporated management's responses to the issues in the "Views of Responsible Officials" section of each issue identified in the audit report.

Corrective Action Plan

A Corrective Action Plan (CAP) will be requested approximately 30 days after the audit report is formally received and filed by the Wayne County Commission. If sufficient corrective action is not implemented by DoIT management as requested, a follow-up review may be necessary.

REPORT DETAILS

PURPOSE / OBJECTIVE

The Office of Legislative Auditor General conducted a performance audit of the Department of Information Technology (DoIT), Controls Over Computer Assets. This type of engagement provides an objective analysis to assist management and those charged with governance and oversight. The information contained in this audit report is intended to assist key stakeholders in the improvement of controls within the County.

Our engagement objective was to assess DoIT's controls over the accountability of inventory, authorized assignment, and disposal of computer assets during our scope period.

SCOPE

We conducted this performance audit in accordance with Generally Accepted Governmental Auditing Standards (GAGAS) issued by the Comptroller General of the United States. 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 conclusions based on our audit objectives.

Our engagement scope was initially set to cover the period of October 1, 2018, through June 30, 2020. However, we modified our engagement scope to also cover the remainder of fiscal year 2020 and fiscal year 2021 to incorporate the CARES (Coronavirus Aid, Relief, and Economic Security) Act laptop purchases in our review.

METHODOLOGY

To address the objectives outlined for this engagement, we conducted discussions and walkthroughs with DoIT management to understand the computer inventory management process. We also conducted limited on-site observations at the Guardian Building, and examined the electronic records stored on the department's SharePoint site.

During our engagement, we conducted judgmental and statistical sampling to select computer assets for assessment and verification. We also assessed DoIT controls over technology service request authorizations; physical shipment verifications; computer disposal and sanitization services; and computer inventory management systems.

Finally, we met with DoIT management to discuss our audit issues and recommendations, and to obtain input and concurrence/or disagreement with the report's final conclusions. Management's Comments has been inserted within the report.

BACKGROUND

The DoIT is responsible for providing technology services to all elected officials and departments, which includes the acquisition, distribution, disposal, physical verification, safeguarding, recording and overall accountability of computer assets owned by the County.

The Department of Information Technology (DoIT) was established to provide technical assistance and support to County user departments, divisions, and agencies regarding the design and implementation of integrated data collection, processing, and information development systems. The DoIT was also established to assist user departments in procuring the most current, cost-effective and compatible technology, and to enforce information systems management standards and policies within the County.

The mission of the DoIT is to serve the Wayne County communities by partnering with governing bodies, providing a passionate commitment to purposeful, value driven technology. The department is comprised of three (3) divisions: Enterprise Computing & Infrastructure (ECI); Technology Experience, and Enterprise Applications.

- The ECI division acquires, develops, and deploys innovative technology solutions for County departments and elected offices.
- The Technology Experience division manages the procurement and management of technology assets to maintain the continuity of business operations.
- The Enterprise Applications division acquires, develops, and deploys innovative software solutions to maximize efficiencies.

Tech Refresh Program

Wayne County officials implemented a strategic plan to replace older computer equipment in accordance with IT industry standards. The IT industry standards currently recommend for large enterprises to replace between 25% to 33% of technology hardware assets (i.e., desktops and laptops) each year due to ongoing changes to technology.

As a result, DoIT established a Tech Refresh Program to replace a portion of the older computer equipment on an annual basis. Per this program, standard desktop computers are to be replaced every five (5) years, and standard laptop computers are to be replaced every three (3) years. DoIT currently is appropriated $1.2 Million of funding each year to execute the Tech Refresh Program.

Ivanti Service Management

DoIT purchased the Ivanti Service Management system during fiscal year 2018, to better manage incoming service desk tickets, and to help improve the department’s computer asset management capabilities, change management functionality, and reporting abilities.

- DoIT has since leveraged the reporting capabilities of the Ivanti Service Management system to assist in the monitoring and tracking of computers that have been deployed to departments and elected offices. DoIT has utilized the technology to generate an Ivanti Ping Report to monitor and manage computers that are logged into the county’s network.

- DoIT has also realized operational efficiencies in the processing of help desk tickets with the Ivanti Service Management system. The department is now able to close out 91% of incoming help desk tickets within one business day.

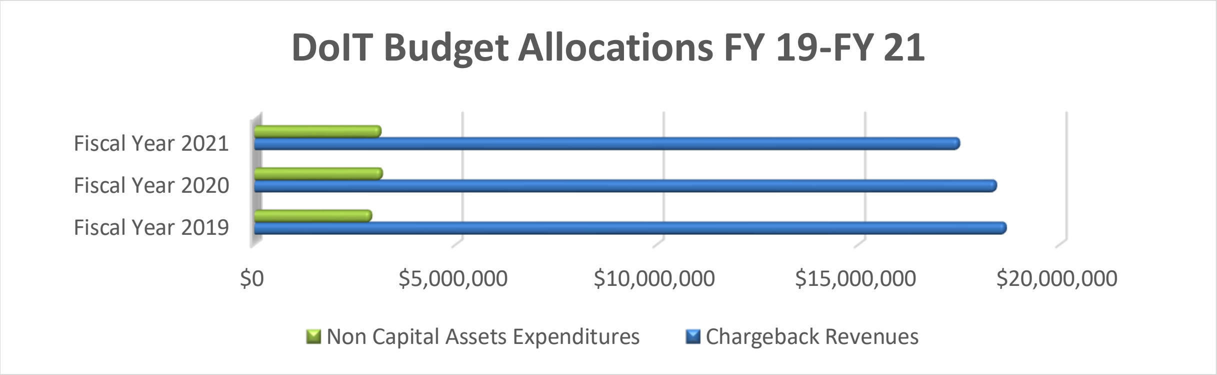
DoIT recently renewed its contractual agreement with Ivanti Inc. for the period of October 1, 2021, through September 30, 2024, to continue usage of the Ivanti Service Management system.

Computer Disposal and Sanitization Services

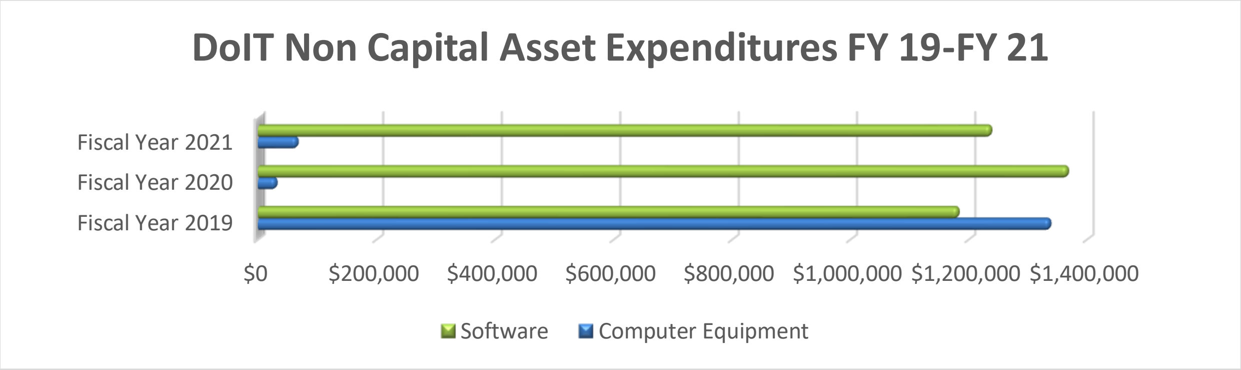
DoIT is also responsible for selecting computer asset disposal vendors for the County. The department currently awards service contracts to disposal vendors that have R2/RIOS Certification and provide the most affordable costing. In December 2019, the County entered into an agreement with a vendor to provide disposal pick-up, recycling, and hard-drive sanitization services for a nominal charge. However, during FY 2022, DoIT is currently developing a formalized RFP/RFQ bidding process to ensure that a fair and equitable process is followed going forward.

Financial Activity

During fiscal years 2019 through 2021, Wayne County Officials appropriated roughly $18 Million of chargeback revenue to Fund 635 Central Services, Information Technology Account for internal operations. About $3 Million of these annual dollars were budgeted for Non-Capital Asset expenditures (i.e., software and computer equipment purchases) (See Chart Below).



During fiscal year 2019, approximately $1.3 Million of expenditures were incurred for computer equipment purchases, and approximately $1.2 Million were incurred for software purchases. However, DoIT's computer equipment expenditures substantially declined to $29,000 in fiscal year 2020, and to $65,000 in fiscal year 2021, while software purchases remained consistent (See Chart Below).



During fiscal year 2020, the County received over $209 Million of CARES Act grant funding, as part of COVID-19 relief. County officials subsequently established Fund 298, COVID-19, Non-Capital Assets to account for computers purchased with these funds. Approximately $1.04 Million of these grant funds were allocated to the DoIT department for the purchase of one-thousand laptop computers for County employees to allow the County to continue providing services through employees working remote.

DoIT expended approximately $442,000 of these grant funds on computer equipment during fiscal year 2020, and approximately $159,000 of these grant funds on computer equipment during fiscal year 2021.

OBJECTIVE: ASSESS DOIT CONTROLS OVER THE ACCOUNTABILITY OVER INVENTORY, AUTHORIZED ASSIGNMENT, AND DISPOSAL OF COMPUTER ASSETS.

We assessed the Department of Information Technology's internal control environment to verify whether management developed adequate controls over technology service request form approvals; physical shipment verifications; deployment signoffs; monitoring and tracking disposal vendor performance; recording and safeguarding of computer inventory, and establishment of written agreements with vendors.

Conclusion

The Department of Information Technology (DoIT) stores a significant portion of their computer assets that are waiting for deployment in a room located on the Mezzanine floor. Along with the Mezzanine area, DoIT maintains computer inventory within its department. We noted DoIT has established effective controls over Mezzanine badge access rights, as all badge access granted to County employees and contractors to enter the inventory areas appeared to be appropriate per work assignments with the County. However, we determined that DoIT needs to strengthen controls (in the following areas) over the management of computer inventory:

- Policies and procedures to maintain continuity of business operations
- Written contractual agreements with disposal vendors
- Monitoring and review of disposal vendor performance
- Tracking and recording of computer inventory in Ivanti
- Storage and retention of departmental records in a centralized location
- Storage of computer inventory awaiting distribution and/or disposal

Below are the specific conditions along with corresponding recommendations that we identified to manage and mitigate risks within the computer inventory management process:

Enhance Policies for DoIT Operational Procedures

Written policies and procedures are critical to ensure management's prescribed policies for safeguarding and accounting for computer assets are communicated to staff and consistently followed.

The ISO/IEC Information Technology Code of Practice recommends for organizations to establish policies and procedures for all information security processes throughout the entity. Per the guidance, informational security policies and procedures should be well defined, approved by management, communicated to employees and relevant external parties, and reviewed in planned intervals and/or as significant changes occur in business operations.

To obtain a better understanding of DoIT business processes over the management of computer asset inventory, we requested DoIT management provide any policies and procedures that outlines the current computer asset inventory management process and procedures. In response, DoIT management provided us a copy of the Wayne County Issued Laptop Policy that was issued on December 4, 2020.

DoIT management stated that the department has not formalized their computer asset inventory management process into written policy and procedures; however written procedures were currently in development and expected to be completed by April 30, 2021. As of this report date, management has indicated that policies and procedures have been finalized.

By not formally documenting computer asset inventory management processes could lead to inconsistency in operational processes for the department. More importantly, a lack of policy and procedures, including assigned and delegated personnel within the operational procedures, reduces accountability and could expose the computer assets to loss and misappropriation.

Recommendation #2020-01 – Control Deficiency

To mitigate risks related to the management and oversight of computer asset inventory, we recommend DoIT management perform the following:

a) Establish and adopt comprehensive policies and procedures for the computer asset inventory management processes, including but not limited to: the acquisition, distribution, disposal, physical verification, safeguarding, and recording of computer assets. in the Ivanti inventory management system, and stand-alone database repositories (i.e., procurement database).
b) Develop a periodic review process of DoIT policies and procedures to ensure that current policies and procedures address any changes to current business practices and/or external standards.

Views of Responsible Officials

Management Agrees with the Recommendation(s)

The Department of Information Technology plans to refocus on the Policies and Procedures area within the department.

Establish Written Agreement With Disposal Vendor

The ISO/IEC Information Technology Code of Practice recommends for organizations to establish a written contractual agreement with any third-party vendor that provides outsourced information security services (i.e. destruction of hard drives). Per the guidance, organizations are responsible for ensuring that contractual obligations for information security services are thoroughly communicated and understood by all parties through a written contractual agreement.

To assess the adequacy of controls over disposal vendor contracts, including whether controls were developed to effectively monitor vendor performance and compliance to contractual agreements (i.e. vendor performance reports), we requested DoIT Management provide a copy of any written contracts held with vendors who perform the electronic disposal services during our scope period of October 1, 2018 through current.

DoIT Management informed us that the current vendor was selected by the County in late 2019 to provide computer equipment disposal services due to their lowest cost and R2 certification status. However, DoIT management has not established a written contract with the vendor and indicated that the department currently has an agreement with the vendor.

According to DoIT Management, because the county only performs a few disposals per year, the department did not draft any performance measures for the disposal vendor during our audit scope period. An assigned DoIT technician performs on-site verification of the computer equipment intended for disposal at the time of pick-up; however, no additional verification or monitoring is performed over vendor performance.

We determined the disposal vendor does in fact provide a destruction certificate, but it only acknowledges the total weight for a particular equipment disposal. We found the certificate provided does not itemize or identify the equipment that was destroyed. As a result, the county has no method to ensure "all" the computer assets provided were destroyed.

DoIT Management also stated services provided by the disposal vendor initially provided for computer equipment pick-up, recycling, and hard-drive sanitization services to the County free of charge. However, the vendor began to charge the County for certain disposals due to the type of equipment retrieved (i.e. printers and fax machines).

While DoIT Management acknowledged the department has not established a formal monitoring process over the disposal vendor's performance and compliance to any requirements of the agreement (i.e. performance reports), management stated a formal RFQ bidding process will be used to select disposal vendors on a go forward basis.

Without a written contractual agreement with the disposal vendor, the County may be unable to monitor vendor performance and assess compliance with the agreement. More so, presently, the County may also be unable to obtain legal restitution for any breaches of the agreement, such as instances of poor vendor performance and/or gross negligence, that could expose county information contained on the computers.

Recommendation #2020-02 – Control Deficiency

To mitigate risks related to the administration and monitoring of disposal vendor services, we recommend DoIT management:

a) Ensure that a written contractual agreement is established with the new disposal vendor that details the specific services to be performed and reporting requirements.
b) Ensure detailed information (i.e., serial number) on each asset destroyed is provided by the vendor on its destruction certificate for reconciliation with county records.
c) Monitor and review disposal vendor performance and compliance to all required processes and procedures to perform the services, including annual certification audits conducted by third party.
d) Consider conducting periodic on-site observation of the vendor's destruction process.

Views of Responsible Officials

Management Agrees with the Recommendation(s)

The Department of Information Technology issued a Request for Proposal (RFP) for disposal services in 2021. The RFP has been awarded to a vendor and the contract is working its way through the purchasing process.

Improve Record of Hard Drive Sanitization

We obtained from the National Institute of Standards and Technology (NIST) a sample Certificate of Sanitization. This agency is recognized for providing guidelines for advancing IT standards, functions, and services. We noted that the NIST certificate identifies detailed information regarding the person performing the sanitization, detailed equipment information including the serial number, and the method of media sanitization.

Based on discussions with the Department of Information Technology management, Wayne County employees' computer hard drives are not sanitized (i.e. destroyed) prior to vendor pick-up for computer asset destruction. Under current practices, DoIT requires the disposal/recycling vendor to physically destroy all types of hard drives from county business units including elected officials.

To conduct the destruction, DoIT schedules the disposal, provides the disposal vendor with a disposal listing of computer assets, and instructs the vendor to pick up the items either directly from a county business unit or a central location within a county building for a consolidated disposal pickup. An assigned DoIT technician performs on-site verification of the computer equipment intended for disposal at the time of pick-up.

We inquired whether the hard drives within the computer assets are erased, either by using software or shredding, prior to destruction to eliminate any county sensitive/confidential information being exposed. According to DoIT management, they stated it was not cost-effective for the county to physically destroy the hard drives nor did they have the staffing available to perform this task.

We also requested Management to provide a sample Certificate of Recycling from the disposal vendor for a destruction dated December 18, 2019. We determined after disposal, the vendor provides DoIT with the Certificate of Recycling, and a copy of the disposal listing which is signed by a DoIT employee to verify that the items were picked up.

However, we determined the Certificate of Recycling only indicated the total weight of all items disposed in each category, such as computers, printers, etc. The certificate did not contain enough detailed information (i.e., serial number) to reconcile to the disposal listing provided to the vendor. We noted that the Certificate of Recycling did not include the following:

- Certify that the hard drives were shredded/destroyed.
- Indicate the method of destruction.
- Record the serial numbers of the recycled computers; or,
- State the number of hard drives destroyed.

Based on our assessment, we determined DoIT has not established a process to ensure computer hard drives are sanitized prior to the vendor's pickup of computer assets identified for disposal. According to DoIT management, the process of erasure and degaussing (magnetic erasure) have been proven as ineffectual. In addition, based on discussion with management they are implementing a RFQ process to obtain vendor disposal services including hard drive destruction.

While DoIT relies on the Certificate of Recycling to maintain compliance with privacy laws, DoIT cannot ensure that all County hard drives are destroyed based on the information provided on the Certificate of Recycling. In addition, the County cannot perform a reconciliation of computer hard drives destroyed due to the lack of detailed information recorded on the Certificate of Recycling.

Recommendation #2020-03 – Control Deficiency

To mitigate the risk that sensitive information may be exposed after the vendor picks up county computer assets, we recommend the Department of Information Technology perform the following:

a) Ascertain, on a cost-benefit analysis, if a process can be implemented to destroy the hard drives prior to the disposal vendor pick-up of county computer assets.
b) Ensure the vendor provides within its Scope of Services a Certificate of Destruction and includes the successful shredding of County hard drives.
c) Ensure the vendor certificate of destruction includes the computer asset serial number, method of destruction, date of destruction, and the number of hard drives disposed.

Views of Responsible Officials

Management Agrees with the Recommendation(s)

The Department of Information Technology will include detailed steps vendors must follow in the destruction of hard drives in the RFP for disposal services that is being developed. These steps include:

- Shred hard drives to render them fully unusable and inaccessible
- Document hard drive serial numbers and associated computer asset tag information
- Provide a certificate of disposal

<u>Conduct Periodic Inventory Checks</u>

In accordance with Wayne County Department of Management and Budget (M&B) Policy No. 12000, computer assets valued at less than $5,000 are classified as a controlled asset. Per the policy, the Wayne County Department of Information Technology (DoIT) is required to perform an inventory verification of all county-controlled computer assets on an annual basis to ensure that all assets are properly classified and described in the inventory log.

The County was appropriated several million dollars CARES Act funding for county operations as a result of the pandemic. The DoIT was able to utilize CARES funding to purchase 1,000 laptops to be utilized by employees. Based on the CARES Act laptop report dated July 14, 2021, we noted that approximately 354 of the 1,000 laptops were distributed to user departments between October 15,2020 and June 16, 2021. The remaining 646 laptops are awaiting deployment to county business units.

In order to assess accountability over computer assets after deployment, we judgmentally selected a sample of 50 deployed CARES laptops from 14 business units to verify the delivery of the computer assets. On September 30, 2021, we forwarded emails along with the attached Computer Inventory Verification Forms to the 14 business units, including elected officials. We requested that the user departments verify the laptop's serial number, custodian, and location.

As of October 29, 2021, we received responses from eight (8) of the 14 user departments, which accounted for 31 of the 50 CARES laptops. For the other six (6) user departments, we attempted to determine whether the remaining 19 computers were in use by an employee within the assigned business unit based on a review of the Ivanti Ping Report dated September 15, 2021. If the computer asset tag and/or custodian was not located within the Ping Report, we requested a copy of the Deployment Form from DoIT to verify that a custodian signed for the laptop at the time of distribution.

For the 31 laptops identified within the business units, we were:

- Able to confirm 24 were verified by county officials within the business units;
- Unable to verify seven (7) CARES laptops identified by DoIT as being within the respective business unit. However, based on our subsequent review of the Ping Report, we were able to verify that two (2) of the seven (7) laptops were being used by an employee within the identified business unit although we were not provided deployment forms.
    - For the remaining five (5) laptops not confirmed by business units, DoIT provided documentation for four (4) of the deployed laptops.
    - According to DoIT, one (1) laptop did not have signed deployment forms on file.
        - However, on March 16, 2022, DoIT provided an email stating that the asset tag number was transposed on the CARES listing for another identified laptop. However, we were able to trace both asset tag numbers (J210498 and J210489) to an invoice and packing slip. As a result, to date we have not received a deployment form for asset tag #J210498. Therefore, the laptop is still deemed unaccountable.

For the remaining 19 laptops identified within the six (6) nonresponsive business units, we determined:

- Six (6) laptops were verified from deployment forms provided by DoIT;
- Twelve (12) laptops were in use by the business units based on our review of the Ping Report dated September 15, 2021; although we were not provided deployment forms.
- However, DoIT was unable to provide a signed deployment form for one (1) laptop.
    - Subsequently, on March 16, 2022, DoIT provided a SharePoint link to a deployment form with a stamped signature from the Custodian dated March 7, 2022. We assert because stamped signatures should not be allowed to substitute for the Custodian's handwritten signature, and the deployment form was signed nine (9) months after the deployment date, we deem this one laptop as still unaccounted for.

In summary, we determined for the 50 laptops sampled:

- 48 were confirmed as delivered to a county business unit, although a signed deployment form was not always obtained at the time of delivery.
- DoIT was unable to provide supporting documentation of delivery for one (1) laptop, asset tag #J210498.
- DoIT provided a deployment form with an electronic signature, dated nine (9) months after the deployment date for one (1) laptop; as such this laptop is deemed unaccounted for.

Based on discussions with management, DoIT does not perform an annual inventory verification with user departments as required in M&B Policy No. 12000. Instead, DoIT relies on its security and asset management software, Ivanti, to periodically generate a “Ping” report that identifies the location of the laptop. According to DoIT, the laptop is programed to produce a “Ping” signal when the device is powered on and connected to the Internet. However, if the device is not powered on, DoIT does not have a compensating control to ensure that the computer asset is in the County’s possession after its distribution.

According to DoIT management, a lack of manpower within the department makes it impossible or not cost effective to perform a county wide manual inventory check. Furthermore, DoIT has recently developed a new method to manage computer inventory while the County is working semi-remotely.

Without validating, periodically, the physical location of computer assets, the County cannot ensure that computer laptop and desktop assets, which may contain confidential and sensitive data, have not been misplaced, lost or stolen. In addition, failure to perform periodic verification with county business units could result in unreliable inventory records due to computer assets not being accounted for.

Recommendation #2020-04 – Control Deficiency

To comply with M&B Policy No. 12000 and strengthen controls over computer assets that cost less than $5,000, we recommend DoIT management develop a county wide inventory policy to include, but not limited to, the following:

a) Require county business units, in accordance with M&B Policy, perform a physical inventory count of computer assets (laptops, desktops), at least annually, and forward a written report to DoIT for review and reconciliation to their records.
b) During the distribution process, ensure that every county employee assigned to a computer asset provides a handwritten signature and date on an attestation form adhering to their accountability over the assigned asset and financial responsibility for its loss.
c) DoIT develop a standard inventory checklist to be used by the business units during their internal inventory process. The checklist should include the computer’s asset tag, serial number, custodian name, location, and the date of the inventory validation.

d) DoIT perform a comparison of the inventory count/attestation provided from the county departments/business units to the Ivanti inventory file and follow-up on noted exceptions.
e) DoIT should also perform a monthly review of Ivanti to identify computer assets that have not reported to the system for more than two weeks and ascertain the asset's location and custodian.

Views of Responsible Officials

Management Agrees with the Recommendation(s)

The Department of Information Technology agrees with the findings and will work towards implementing the suggested corrective actions.

Strengthen Controls Over the Management of Computer Inventory

Wayne County Department of Information Technology, Facility Security Policy, states "that DoIT is responsible for protecting its facility, equipment, and offices spaces. DoIT must provide physical access control for its facilities and computer systems."

To determine whether DoIT has established adequate controls to record and track the physical location of computers that are stored/held by DoIT prior to distribution, we requested DoIT provide a comprehensive listing of all computers that were purchased and/or recorded during our audit scope period. For our testing, DoIT management provided a system report titled Active Installed. From this list we judgmentally selected a sample of 70 computers. These computers consisted of both laptop and desktop computers that had not been deployed to county business units.

We also requested a listing of computer assets recently purchased with Cares Act funds. From this purchase of 1000 laptop computers, we determined that 646 laptops had not yet been deployed to county personnel. From the list of 646, we statistically selected a sample of 65 laptops, or 10 percent, to test whether adequate controls were in place to record and track their physical location.

To assess the inventory of the selected sample of 135 undistributed computer assets, we performed an onsite verification on November 18, 2021 and December 17, 2021 at the Guardian Building. The samples were located on two floors at the Guardian Building: the 13th floor and a room on the Mezzanine level.

Based on our review, we noted the following observations during our onsite verification procedures:

1. We determined from the group of 70 computer assets on the Active Installed list:
   - 31 of the 70 computer assets were accounted for at the Guardian Building; for the remaining 39, we were unable to identify the location of the assets.
   - We subsequently attempted to locate these 39 computers within the September 2021 Ivanti Ping Report to determine if the computers had been distributed to a department and/or elected office. However, we were only able to locate eight (8) of the 39 computers within the report. Therefore, we requested DoIT management to provide the signed deployment sheets for the remaining 31 computers.
   - DoIT Management was able to provide us a signed deployment sheet for two (2) of the 31 computer assets that we requested. However, to date, management has been unable to provide signed deployment documentation for the remaining 29 computer assets.

2. We determined from the group of 65 computer assets purchased with Cares Act Funds:
   - We identified 34 of 65 computers as accounted for at the Guardian Building. For the remaining 31, we requested copies of deployment/confirmation of receipt forms from DoIT.

- DoIT provided copies of signed deployment forms with employee signature and date of deployment for 21 of the remaining 31 computers.
- We were unable to validate the final disposition for ten (10) of the 31.
  - On March 16, 2022, DoIT provided additional information for the ten (10) laptops. We noted the following:
    - For three (3) of the laptops, DoIT provided deployment forms signed after the date of deployment. In addition, one (1) of the three (3) units had a deployment form signed by someone other than the Custodian of the laptop.
    - Five (5) of the laptops were listed on an unsigned deployment form;
    - One (1) laptop was identified as being in DoIT's custody; and,
    - To date, we have not received a deployment form for one (1) laptop.

In summary, for the 135 computers tested, we have determined 39 of 135 (or 28%) in which DoIT was not able to provide evidence of a signed deployment form and/or the date of the signed deployment form was after the date of delivery to a county business unit.

In addition, although DoIT management had previously indicated that the Cares Act Laptops were only stored in the Mezzanine room, while on site, we observed the following:

- DoIT currently stores computer inventory within five (5) separate locations.
  1. The Mezzanine room, in which computers were stored within laptop cases, on shelving units and tables, and unopened boxes within shipping crates.
  2. The 13th Floor where we found computers located within four (4) separate storage rooms.

Based on our on-site observation of the inventory, DoIT did not appear to have any tracking mechanism to identify the locations of the selected sample of computer assets. Further, although management stated there is restricted badge access as well as security cameras on both floors, we found a lack of physical safeguards over the computer inventory, specially that was stored within the open cubicle workstations, on the 13th floor and within the mezzanine room.

DoIT management stated that prior to the pandemic, the department had a designated staff person to oversee the computer inventory management process; however, this individual was furloughed in May 2020. Therefore, DoIT has been unable to effectively monitor and track the computer inventory that was stored at the Guardian Building during our scope period. DoIT management also stated that the department did not consistently upload all Deployment Sign-off Forms into the SharePoint database during our period of review. Further, DoIT stated personnel manually filed older Deployment Sign off Forms within various locations in the department.

Without an established mechanism to track and account for all computer inventory, DoIT may not be able to effectively account for all computers purchased, received, and deployed. In addition, by not having a centralized storage location of computer inventory that can be effectively monitored, the County may be unable to effectively track and locate all computers that are received, stored, and awaiting distribution. This could result in misplacement, loss, or undetected theft of computer assets (laptops, desktops, etc.).

Recommendation #2020-05 – Control Deficiency

To strengthen the controls and mitigate risks related to the management and storage of computer asset inventory, we recommend DoIT management pursue the following:

a) Establish policy and procedures to formalize a process for recording and tracking all computer inventory that is stored by DoIT and awaiting distribution, including but not limited to,:
   i. Ensure all computers are stored within a centralized location.
   ii. Properly label and identify each computer that is received and placed in storage.
   iii. Ensure that all idle computers are stored within a secured locked room.

b) Ensure DoIT management maintains a written record of all computer inventory received, its location, and retrieved from storage by DoIT personnel for distribution.

c) Periodically conduct a physical verification of the computer inventory that is maintained by DoIT in storage to ensure agreement to inventory records and/or reports.

Views of Responsible Officials

Management Agrees with the Recommendation(s)

The Department of Information Technology has updated Product Intake policy and procedures. The Product Intake process will be an area of focus for our newly hired Asset Manager.

Enhance Documentation Over the Receiving and Distribution Process

GFOA Best Practices for establishing written Policies and Procedures state:

- A description of which employees (by title, as well as the identity of incumbents) are assigned to perform which procedures.
- Explain the design and purpose of control-related procedures to increase employee understanding of and support for controls.

To determine if DoIT established adequate controls over the receipt and distribution of computer purchases, we requested a copy of the Closed Installed Report which, according to DoIT officials, lists computer equipment that has been purchased and installed within county business units. The requested period was from October 2018 through February 2020.

Our assessment was to ascertain whether DoIT retained:

- An approved service request form, purchase order agreement, packing slip(s), and deployment sign-off form(s) acknowledging the computer asset was distributed to county employees/business units.

We met with DoIT management who stated most of the requested documentation was scanned into the SharePoint database management system. From the Closed Installed report, we judgmentally selected a sample of purchase orders that contained 501 computers and reviewed the SharePoint database to verify the receiving and distribution documentation was evident in the system.

Based on our sample testing, we determined the following:

Receiving and Recording

Per our review, we confirmed that the County had received all 501 computers in our sample from our verification of the Service Request Forms, Purchase Orders and the Packing Slips.

- However, we noted that the packing slips that had accompanied the delivery of the 501 computers did not include a signature or initials to indicate verification of receipt by DoIT personnel. Specifically, we found no sign-off or dates were recorded on the receiving documents (i.e., packing slips).

Distribution

1. We judgmentally selected a sample of 14 computers to test from three (3) purchase orders that contained 454 computers that we were not able to locate a deployment form within the DoIT Sharepoint system.

    a. We subsequently reviewed the September 2021 Ivanti Ping Report and were able to locate five (5) of the 14 computers within county business units. However, we were unable to determine the location and assignment for the remaining nine (9) computers that did not have a completed Deployment Sign-off Form on file.

2. We tested the remaining 47 of the 501 computers to verify whether the deployment forms were on file. Based on this assessment we found the following:

    a. We verified 27 of the 47 computers had deployment sign off forms and indicated the computer had been deployed within the year of purchase.

    b. However, we noted the remaining 20 of the 47 computers had Deployment Sign-off Forms that had been signed by the various departments and/or elected offices during the month of November 2021. The November 2021 sign off dates on these forms were two (2) to three (3) years after they were received by the county (i.e. 2018 and 2019).

DoIT management stated that the department did not have a process in place to formally document and sign-off on packing slips once completed. The department personnel would instead note any order discrepancies within the DoIT Procurement Database spreadsheet, and directly contact the supplier for resolution. DoIT management also stated that departmental operations had been adversely impacted due to a mandatory reduction in force in May 2020. Therefore, the department was unable to perform adequate monitoring and tracking of deployment sign-off sheets on a timely basis.

By not having a sign off on packing slips by DoIT Personnel on items purchased from a vendor could lead to discrepancies between the purchase order, invoice and items received. In addition, the County may be unable to effectively monitor and account for computer inventory on hand, due to an inability to consistently obtain and record deployment sign-off forms in a centralized database that would show the locations and assignments of all computer inventory in their possession.

Recommendation #2020-06 – Control Deficiency

To mitigate risks related to the receiving, recording and distribution of computers purchases, we recommend DoIT management establish policies and procedures to:

a) Require a sign-off to be completed by DoIT personnel on receiving (i.e. packing slips) documents for each shipment to verify the quantity received and note exceptions.
b) Ensure that a Deployment Sign-off Form is signed and dated by a representative of DoIT and the requesting department/elected office during the on-site pick-up and/or distribution.
c) Also ensure that all Deployment Sign-off Forms are recorded/stored in a centralized location on SharePoint for third party review.

Views of Responsible Officials

Management Agrees with the Recommendation(s)

The Department of Information Technology agrees with the findings and is working on reviewing and streamlining the deployment process.

OAG OVERALL CONCLUSION

The Department of Information Technology has been effective in meeting its goals and objectives to ensure that County departments and elected offices obtain the most current, cost-effective and compatible technology to conduct their business operations, and for ensuring that Mezzanine badge access rights are properly granted to County employees and contractors.

However, we determined that DoIT management can strengthen controls within the following areas that include but are not limited to: technology service request form approvals; physical shipment verifications; deployment signoffs; monitoring and tracking disposal vendor performance; recording and safeguarding of computer inventory; and establishment of policies and written agreements with vendors.

There were six (6) issues and 20 recommendations made to strengthen controls and processes within the Department of Information Technology (DoIT) operations. All six (6) of the issues are classified as control deficiencies, which are deemed to be low risk.

We discussed the issues and corresponding recommendations with representatives from the Wayne County Department of Information Technology. Management agreed with all 20 recommendations within the six (6) issues. We have included Management's responses to the issues and recommendations within the audit report.

A Corrective Action Plan will be requested approximately 30 days after the audit report is formally received and filed by the Wayne County Commission. If sufficient corrective action is not implemented by management as requested, a follow-up review may be necessary.

This audit report is intended solely for the information and use of the Wayne County Department of Information Technology and the Wayne County Commission and is not intended to be and should not be used by another other than these specified parties. This restriction is not intended to limit the distribution of the audit report, which is a matter of public record.

Sincerely,

Marcella Cora

Marcella Cora, CPA, CIA, CICA, CGMA
Auditor General

Appendix A

Definition of Internal Control Deficiencies

Control Deficiency (low risk)

A control deficiency exists when the internal control design or operation does not allow management or employees, in the normal course of performing their assigned functions, to prevent, detect or correct errors in assertions made by management on a timely basis. A deficiency in design exists when (1) a control necessary to meet the control objective is missing or (2) an existing control is not properly designed so that, even if the control operates as designed, the control objective is not met.

A deficiency in operation exists when a properly designed control does not operate as intended, or when the person(s) performing the control does not possess the necessary authority or qualifications to perform the control effectively.

Significant Deficiency (medium risk)

A matter that, in the auditor's judgment, represents either an opportunity for improvement or significant deficiency in management's ability to operate a program or department in an effective and efficient manner. A significant deficiency in internal control, or combination of deficiences, that adversely affects the organization's ability to initiate, authorize, record, process or report data reliably in accordance with applicable criteria or framework such that it is more than a remote likelihood that a misstatement of the subject matter that is more than inconsequential will not be prevented or detected.

Material Weakness Deficiency (high risk)

A significant deficiency that could impair the ability of management to operate the department in an effective and efficient manner and/or affect the judgment of an interested person concerning the effectiveness and efficiency of the department. A significant or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of subject matter will not be prevented or detected.