HARFORD COUNTY, MARYLAND
Office of the County Auditor

AUDIT OF ICT INVENTORY CONTROLS

Report Number:
2025-A-07

Report Date:
2/3/2025

Council Members and County Executive Cassilly:

In accordance with Section 213 of the Harford County Charter, we have performed an audit of Information and Communication Technology Inventory Controls for the period of 7/1/2023 through 9/30/2024. This audit was conducted as part of the County Auditor's risk-based Annual Audit Plan approved by the County Council for FY2025.

The objective of the audit was to determine if the County's Department of Information and Communication Technology (ICT) has adequate controls in place to ensure that inventory is properly protected from loss and can be accounted for. The scope of this review was limited to ICT's inventory control processes and did not include a complete review of inventory included in the County-wide inventory system or the related County-wide processes. The results of the audit, our findings and recommendations for improvement are detailed in this report.

We would like to thank the members of management for their cooperation during the audit; they have been provided an opportunity to respond to this report; the responses provided follow the Issues and Corrective Actions.

Sincerely,

Chrystal Brooks, CPA

Chrystal Brooks
County Auditor

CONCLUSIONS

Our conclusion, based on the evidence obtained, is that computer hardware, network equipment and other inventory items are tracked and protected, but the inventory lists have not been updated consistently. This assessment is based on the strengths and weaknesses identified for the operational objectives below.

Business Process Objective	Assessment[i]
Inventory/ Equipment is properly tagged and tracked	Generally Effective
Inventory is held securely	Effective
Inventory/ Equipment is disposed properly	Effective

ISSUES AND CORRECTIVE ACTIONS

2025-A-07.01 Items could not be located

According to the County's Capital Asset Management policy FO-03, "Facilities & Operations will maintain a list containing a current description and location for all County data-sensitive electronic assets with a minimum market value of $100.00 or other Capital Asset with a minimum fair market value of $500.00." Inventory items are generally purchased, tagged, and logged into the inventory system, AssetWorks, by Department of Information and Communication Technology (ICT) employees.

Management provided inventory lists including 12,884 technology assets that are managed by ICT (2,710 items) or assigned to other departments (10,174 items). We sampled items from the lists, to confirm each item's physical existence, that its location matches the inventory report, the inventory is tagged, and, if applicable, proper removal from inventory records and disposal of the item. Of the 90 items sampled, 19 either could not be located or AssetWorks lacked enough information to determine how to track down the item.

Based on our review of the inventory lists provided and discussions with management, it appears that numerous items were input years ago and integrated into AssetWorks either without sufficient identifiable detail and/or proper transfer protocol was not followed. Inventory turnover, refreshes, and updates are inherent in the use of technology. Consequently, without adequate and consistent adherence to inventory procedures, including sufficient detailing of items, there is a risk that inventoried items are no longer available for use either because they were lost, transferred, or surplussed. Further, it is inefficient to continue to track items that are obsolete technology.

We recommend, supplemental to the annual County-wide inventory review, ICT perform periodic inventory reviews to ensure records are current, obsolete or immaterial items are removed from tracking, and inventory item detail is sufficient so that items are readily identifiable, easily located, and assigned when appropriate.

Management Response: This audit sampled 90 assets out of 12,884 provided by F&O. The 19 assets that could not be located are shared among County Departments and other agencies, such as the Volunteer Fire Companies. The County will explore policies to govern shared assets with external agencies to ensure appropriate accountability and compliance. In addition, the County currently conducts annual reviews of inventory to ensure records are up-to-date and plans to do the next review at the beginning of the next fiscal year. The County does not depreciate assets and continues to track Capital Assets over a $15,000 threshold, regardless of age and use, until such time as the Capital Assets are removed from

the inventory for surplus and disposal (Policy F&O-03). Assets below the $15,000 threshold are also maintained on the inventory without depreciation, to maintain consistency in the inventory process.

Expected Completion Date: 9/1/2025

BACKGROUND, OBJECTIVES, SCOPE, AND METHODOLOGY

The Department of Information & Communication Technology (ICT) is responsible for information systems administration, applications development, network management, telephone and email connectivity, and hardware and software technical support for numerous systems County-wide. In order to operate and maintain the County's network infrastructure, hardware, and software, as well as service County employee technology-related needs, ICT must have available thousands of pieces of equipment.

ICT follows the County-wide inventory policy. That policy requires items over $500, and data sensitive electronics over $100, to be given a county inventory number. ICT is partially or fully responsible for the acquisition, maintenance, and disposal of nearly 13,000 technology items assigned to County employees used in the completion of their work. All of these items require general oversight and periodic tracking. ICT accomplishes this using the County's inventory management system, AssetWorks, in conjunction with Facilities & Operations, and with internal spreadsheets.

The audit approach focused on testing the key controls that address management's objectives. Our audit procedures included interviewing personnel, observation and testing as described in the table below.

Process / Control Objective	Scope of Review
Inventory Tracking	
Items can be found in their assigned storage locations and/or with an assigned person.	• For a sample of items in the inventory lists, observe their existence at specific facilities.
High cost or sensitive equipment is given an asset tag when purchased.	• Search for computer hardware and network equipment purchases that should be included in inventory and for a sample of transactions, confirm items were tagged and recorded. • At various facilities, select a sample of items to confirm that they have been included in the inventory lists.
An annual inventory confirmation is performed.	• Compare inventory lists to determine that they contain consistent, up-to-date information.

Process / Control Objective	Scope of Review
	• Confirm routine reviews and evaluations of inventory are performed, reconciliations occur, and identified issues are corrected.
Items over $500 are captured in the County-wide inventory management system and given asset tags.	• For a sample of items observed on site, confirm they were recorded in the inventory records.
Physical Security	
Inventoried items are kept in locations with limited access.	• Observe the physical security controls where items are stored. • Review access reports for selected areas to confirm that access is restricted to appropriate and necessary current staff and vendors.
Surplus and Disposal	
Disposal of equipment is reviewed and approved prior to being removed from inventory	• Determine if inventory items are surplussed and disposed are authorized using properly completed forms according to County policy.

Areas for improvement are described in the Issues and Corrective Actions section of this report. There were no prior audits of this subject matter.

Harford County management is responsible for establishing and maintaining effective internal controls. Internal control is a process designed to provide reasonable assurance that objectives pertaining to the reliability of financial records, effectiveness and efficiency of operations including safeguarding of assets and compliance with applicable laws, rules and regulations are achieved. Because of inherent limitations in internal control, errors or fraud may nevertheless occur and not be detected.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Report Distribution:	Audit Team:
Mr. Nicholas Kuba, Director, Information and Communication Technology Mr. Robert McCord, Director of Administration	Chrystal Brooks CPA, CIA, CGAP, CISA, CGFM, CRMA *County Auditor* Brad DeLauder CPA, CIA *Senior Auditor*

---

[i] Definitions

Effective: The design and effectiveness of the internal control environment address key risks. The business unit complies with external laws and regulations, and internal policies, procedures and guidelines. Business processes are managed effectively resulting in achievement of expected outcomes.

Generally Effective: The design and/or effectiveness of the internal control environment generally address key risks; however, the number and severity of findings relative to the size and scope of the business unit being audited indicate that some minor areas of weakness in the control environment need to be addressed. Isolated instances of non-compliance with external laws and regulations, and internal policies, procedures and guidelines may exist. Business processes may not be managed effectively in all areas resulting in reduced achievement of expected outcomes.

Not Effective: The design and/or effectiveness of the internal control environment does not address key risks. Non-compliance or historical patterns of non-compliance with key regulatory requirements and internal policies, procedures and guidelines exist which expose the audited entity to financial, reputational, and operational risks. Business processes are not managed effectively and expected outcomes are not achieved.