MEMORANDUM

May 4, 2026

TO: Kevin Cornish, Chief Information Officer
Information Technology Division

Kevin Cathy

FROM: Kevin Cathy, Branch Chief
Program Integrity Division, Office of Audit Services

RE: Information Technology Division – Final Audit Report –
Hardware Asset Management Audit (Assignment #2526.01)

In accordance with the Fiscal Year 2025-2026 Internal Audit Plan that was approved by Covered California's Audit Committee in June 2025, the Office of Audit Services conducted an audit to provide reasonable assurance of the existence and strength of Covered California's internal controls over the Hardware Asset Management process for the period of July 1, 2024, through June 30, 2025. Our report of this audit is attached.

We appreciate the cooperation and assistance of the Information Technology Division's management and staff during our audit. If you have any questions regarding this report, please contact Alicia Watts at (916) 954-3981 or Alicia.Watts@covered.ca.gov.

Cc: Executive Office
Jessica Altman, Executive Director
Kathleen Webb, Chief Deputy Executive Director, Operations
Brandon Ross, General Counsel, Program Compliance & Accountability

Information Technology Division
Shilpa Akunuri, Chief Technology Officer
Linh Thao Huynh, Chief Information Officer
Tina Mitchell, Chief Information Security Officer
Amanda Holmes-Davidian, Information Technology Manager II
Preston Cleary, Information Technology Manager I

Program Integrity Division
Thien Lam, Director
Deepshikha Kumar, Chief Audit Executive, Office of Audit Services
Alicia Watts, Section Chief, Office of Audit Services
Kurt Faubion, Audit Manager, Office of Audit Services
Ramen Gill, Internal Auditor, Office of Audit Services
Rene Lor Eva, Internal Auditor, Office of Audit Services

HARDWARE ASSET MANAGEMENT AUDIT

COVERED CALIFORNIA
INFORMATION TECHNOLOGY DIVISION

FINAL AUDIT REPORT

ISSUED ON:
MAY 4, 2026

PREPARED BY:
COVERED CALIFORNIA
PROGRAM INTEGRITY DIVISION
OFFICE OF AUDIT SERVICES

AUDIT TEAM:
DEEPSHIKHA KUMAR, CHIEF AUDIT EXECUTIVE
KEVIN CATHY, BRANCH CHIEF
ALICIA WATTS, SECTION CHIEF
KURT FAUBION, AUDIT MANAGER
RAMEN GILL, INTERNAL AUDITOR
RENE LOR EVA, INTERNAL AUDITOR

Table Of Contents

Executive Summary

Objective and Scope

The Office of Audit Services conducted an audit to assess the Information Technology Division's (ITD) effectiveness in managing Covered California's IT hardware asset tracking and inventory processes for the period of July 1, 2024, through June 30, 2025.

Positive Observations

- ITD successfully implemented an IT hardware asset tracking system, ensuring accountability, efficiency, and improved oversight of IT hardware assets within Covered California's operations.

- ITD adhered to proper disposal practices for IT hardware assets, aligning with Covered California's strategic pillar of Organizational Excellence and demonstrating operational responsibility.

Reportable Condition(s)

We noted some matters below that we consider to be reportable under the *Global Internal Audit Standards*:

- A defined frequency has not yet been established for how often all IT hardware assets should be inventoried.

- The IT hardware asset tracking system did not consistently reflect accurate custody and return status of assets.

- The IT hardware asset tracking system contains invalid, duplicate, and incomplete data.

Follow-up

The Office of Audit Services will follow up with management on their progress of corrective action plans and will report updates accordingly to the Audit Committee.
A follow-up audit may be performed to determine the completion and adequacy of the corrective action plans.

Background, Objective, Scope, and Methodology

Background

Covered California's Information Technology Division (ITD) is comprised of the Information Security Office (ISO), Consumer Experience, Data, Strategy, & Portfolio Management, and Employee Experience, Service Delivery, Infrastructure & Operations. These program areas within ITD provide technology acquisition, design, development, and support, program and project management, and information security services. Together, they support Covered California's business operations, including health plan eligibility determination and enrollment, delivery of the enterprise strategic plan, business process optimization, applied innovation, and oversight of the California Healthcare Eligibility, Enrollment, and Retention System (CalHEERS).

The Employee Device Management Team (IT Asset Team), within Employee Experience, Service Delivery, Infrastructure & Operations, manages IT hardware asset tracking and inventory processes. The IT Asset Team is responsible for overseeing hardware and software assets to ensure security, performance, and compliance with organizational policies. Key responsibilities include maintaining asset records and supporting compliance efforts. To manage physical IT assets, ITD uses an IT hardware asset tracking system that tracks and optimizes the lifecycle of these assets. The system enhances visibility and control over inventory, supports compliance, reduces waste, and improves asset utilization.

Objective

The objective of this audit was to assess ITD's effectiveness in managing Covered California's IT hardware asset tracking and inventory processes.

Scope

The scope of this audit covered ITD's oversight of the IT hardware asset management process during the period of July 1, 2024, through June 30, 2025.

Methodology

Our evaluation included gaining an understanding of the hardware asset management process. Additionally, we conducted verification processes to ascertain if the hardware asset management process, internal controls, and resources were effective, efficient, and followed relevant policies, procedures, security standards, and requirements.

Results

Positive Observations

During our review, we evaluated various aspects of the hardware asset management process. We were able to ascertain, with reasonable assurance, the following areas where internal controls were found to be effective:

- ITD successfully implemented an IT hardware asset tracking system, ensuring accountability, efficiency, and improved oversight of IT hardware assets within Covered California’s operations.

- ITD adhered to proper disposal practices for IT hardware assets, aligning with Covered California’s strategic pillar of Organizational Excellence and demonstrating operational responsibility.

Findings & Recommendations

Finding #1 – A defined frequency has not yet been established for how often all IT hardware assets should be inventoried.

Finding Rating:	Priority	High	Medium	Low

Condition
We reviewed ITD's process for conducting system component inventories, which involves reviewing and updating a comprehensive record of all IT hardware assets and their key details (e.g., location, ownership, and status).

We identified that ITD did not formally establish a defined frequency for how often they should conduct system component inventories. Instead, ITD conducts these inventories every two to three years, when directed by the Business Services Branch. The most recent system component inventory was reviewed and updated in December 2023.

Criteria
California Government Code, section 11549.3(f) states, in part, "Every state agency shall adopt and implement information security and privacy policies, standards, and procedures that adhere to *NIST 800-53 Revision 5*."

NIST 800-53 Revision 5, CM-8: System Component Inventory requires organizations to define the frequency for reviewing and updating the system component inventory.

Cause
During the audit period, ITD had yet to establish formal policies and procedures for tracking IT hardware assets, which would have included defining how often system component inventories should be reviewed and updated.

Effect
By not establishing formal policies and procedures for tracking IT hardware assets, that include a formally defined frequency requirement for how often to review and update system component inventories, Covered California could be exposed to potential risks, such as non-compliance with *California Government Code* and *NIST* requirements, unauthorized access, data breaches, inaccurate asset data, and loss of critical assets.

Recommendation
ITD should establish formal policies and procedures for tracking IT hardware assets, which should include a formally defined frequency requirement for how often system component inventories should be reviewed and updated.

Finding #2 – The IT hardware asset tracking system did not consistently reflect accurate custody and return status of assets.

Finding Rating:	Priority	High	Medium	Low

Condition

We reviewed a sample of 10 Covered California employees who collectively had 45 IT hardware assets assigned to them in the IT hardware asset tracking system. As shown in the table below, we identified discrepancies between the system records and actual asset status. Specifically:

- Two assets were recorded as "In Use" by certain employees; however, those assets were in the possession of different employees.
    - Additionally, neither asset had a completed equipment issue form on file.
- Five assets had been returned by employees but were still reflected as "In Use" in the system.
    - Additionally, four assets did not have a completed equipment return form on file.

Asset	Tracking System Status	Actual Status	Equipment Issue/Return Form Completed?
iPad	In Use - assigned to different employee	In Use - by unassigned employee	No
Docking Station	In Use - assigned to different employee	In Use - by unassigned employee	No
Computer	In Use	Returned	No
Computer	In Use	Returned	N/A (test device)
Mobile Phone	In Use	Returned	No
Docking Station	In Use	Returned	No
Docking Station	In Use	Returned	No

Criteria

NIST 800-53 Revision 5, CM-8: System Component Inventory requires organizations to develop and document a detailed inventory of system components that accurately reflects the system.

Covered California Administrative Manual, section 2-602: Inventory Control states, in part, "All Covered California major assets shall be identified and maintained in an appropriate inventory management system managed by BSB and ITD."

Onboard and Offboard Processes for IT Asset Team states, in part, "Deployed or returned equipment is documented in an equipment form via Docusign."

Cause
ITD has documented procedures for issuing and returning equipment. The procedures involve coordination between two teams: the IT Asset Team and the Service Desk Team. However, the procedures were not consistently followed. Specifically:

- The Service Desk Team did not consistently confirm equipment issuances or returns using the required hardware form.

- The IT Asset Team did not consistently verify completed hardware forms and update the IT hardware asset tracking system.

Effect
Inaccurate tracking and missing documentation of issued and returned IT hardware assets could lead to lost, misplaced, or misused assets. Additionally, untracked equipment could result in security risks such as data breaches or unauthorized access.

Recommendation
ITD should explore opportunities, such as automation of certain processes, revising established procedures, and enhancing oversight of both the IT Asset Team and Service Desk Team, to strengthen its existing procedures in order to improve the accuracy and documentation of IT hardware asset tracking.

Finding #3 – The IT hardware asset tracking system contains invalid, duplicate, and incomplete data.

Finding Rating:	Priority	High	Medium	Low

Condition

During our review to assess whether the data within the IT hardware asset tracking system was valid, accurate, and complete, we identified a total of 689 data discrepancies, as detailed in the table below.

Data Field Discrepancy	Total Asset Data Entries Requiring this Data Field	Number of Data Entries with Discrepancy	Asset Details
Invalid/Duplicate Data	N/A	624	Virtual Machines - not IT hardware assets: 540 Mobile Phones - not part of inventory: 6 Duplicate Data Entries: 78
Missing Building Location	4,690	50	Servers: 23 Windows Servers: 13 TVs: 7 Computers: 3 IP Switches: 2 Mobile Phones: 2
Missing Asset Tag Number	4,565	13	Windows Servers: 13
Missing Device Owner	3,792	2	Computers: 2
Total Data Discrepancies		***689***	

Criteria

NIST 800-53 Revision 5, CM-8: System Component Inventory requires organizations to develop and document a detailed inventory of system components that accurately reflects the system, includes all components without duplicates, provides sufficient granularity for tracking and reporting, and to define the frequency for reviewing and updating the system component inventory.

Cause

ITD asserted that the IT hardware asset tracking system configuration and integration with other systems automatically created invalid or duplicate asset records. Additionally, a formal IT hardware asset inventory has not been conducted since before the tracking system's implementation in June 2024. Lastly, during the scope of our review, ITD relied on spot-checks to maintain accuracy and attributed the discrepancies partly due to resource limitations. However, the spot-checking process does not have a defined frequency nor are there written procedures for how to perform them.

Effect
Not having an established process to ensure that data in the IT hardware asset tracking system is valid, accurate, and complete can lead to inaccurate inventories, unreliable data, operational inefficiencies, and complications in tracking, reporting, and decision making.

Recommendation
ITD should establish a formal process that aims to ensure that the IT hardware asset tracking system data is valid, accurate, and complete.

Conclusion

ITD has been actively working to further improve the IT hardware asset management process, particularly by successfully implementing an IT hardware asset tracking system and adhering to proper disposal practices for hardware assets. While some areas demonstrate notable strengths, there are opportunities for improvement, as reflected in the three findings identified during our review. Addressing these findings can help reduce the risk of security vulnerabilities, loss or misuse of critical assets, and inaccurate tracking and reporting. Overall, one finding has been rated as medium risk and two findings as high risk due to the potential adverse effects to ITD’s operations and Covered California as a whole.

Management Response

Presented below is ITD's management response to the findings, which includes their corrective action plans.

Finding 1:	A defined frequency has not yet been established for how often all IT hardware assets should be inventoried.
Recommendation 1:	ITD should establish formal policies and procedures for tracking IT hardware assets, which should include a formally defined frequency requirement for how often system component inventories should be reviewed and updated.
ITD Management Response/ Corrective Action:	ITD Teams are working to build and deploy a policy that will align with ISO and regulatory requirements. This policy will be published and enacted by July of 2026.
Targeted Completion Date:	July 2026

Finding 2:	The IT hardware asset tracking system did not consistently reflect accurate custody and return status of assets.
Recommendation 2:	ITD should explore opportunities, such as automation of certain processes, revising established procedures, and enhancing oversight of both the IT Asset Team and Service Desk Team, to strengthen its existing procedures in order to improve the accuracy and documentation of IT hardware asset tracking.
ITD Management Response/ Corrective Action:	This finding is still being investigated. ITD is looking into the audit trails of all identified assets to identify the most appropriate corrective action. ITD's investigation will be completed by June of 2026, at which time the CAP will be updated.
Targeted Completion Date:	To be determined

Finding 3:	The IT hardware asset tracking system contains invalid, duplicate, and incomplete data.
Recommendation 3:	ITD should establish a formal process that aims to ensure that the IT hardware asset tracking system data is valid, accurate, and complete.
ITD Management Response/ Corrective Action:	As part of the audit policy being developed for Finding #1, missing data will be audited and filled in alongside our hardware inventory process. At present, the process that created duplicate data is being fixed, and other areas of incomplete data are being filled in by the requisite teams responsible for those items.
Targeted Completion Date:	July 2026

Evaluation of Response

The corrective action plans provided by the Information Technology Division, if implemented as intended, should be sufficient to correct the reportable conditions noted. The Office of Audit Services will conduct quarterly follow-ups to provide reasonable assurance that the corrective action plans have been implemented. Additionally, a follow-up audit may be performed to determine the completion and adequacy of the correction action plans.

We thank the Information Technology Division for their help and cooperation during this audit.

Appendix A

Finding Ratings

Finding	Priority	High	Medium	Low
1. A defined frequency has not yet been established for how often all IT hardware assets should be inventoried.		**X**		
2. The IT hardware asset tracking system did not consistently reflect accurate custody and return status of assets.		**X**		
3. The IT hardware asset tracking system contains invalid, duplicate, and incomplete data.			**X**	

Rating Definitions

Priority	Immediate and on-going threat to the achievement of division or Covered California strategic goals and objectives. In particular: - Significant adverse impact on reputation - Non-compliance with statutory requirements - Potential or known financial losses - Substantially raising the likelihood that risks will occur Management must implement corrective actions as soon as possible and monitor the effectiveness.
High	High probability of adverse effects to the division or Covered California as a whole. Management must put in place corrective actions within a reasonable timeframe and monitor the effectiveness of the corrective actions. - High potential for adverse impact on reputation - Increase in the possibility of financial losses - Increase in the likelihood that risks may occur
Medium	Medium probability of adverse effects to the division or Covered California as a whole. Management must put in place corrective actions within a reasonable timeframe and monitor the effectiveness of the corrective actions. - Medium potential for adverse impact on reputation - Potential increase in the likelihood that risks may occur
Low	Low probability of adverse effects to the division or Covered California as a whole, but that represent an opportunity for improving the efficiency of existing processes. Correcting this will improve the efficiency and/or effectiveness of the internal control system and further reduce the likelihood that risks may occur.