COVERED CALIFORNIA

MEMORANDUM

March 17, 2025

TO: Mavilla Safi, Director
Service Center Division

Kevin Cornish, Chief Information Officer
Information Technology Division

Kirk Marston

FROM: Kirk Marston, Chief Audit Executive
Program Integrity Division, Office of Audit Services

RE: Service Center Division & Information Technology Division – Final Audit Report – CalHEERS Manual Override Audit (Assignment #2324.04)

In accordance with the *Government Code*, Section 13400 et seq. and State Administrative Manual, Section 20060, all levels of management must be involved in assessing and strengthening the systems of internal control to minimize fraud, errors, abuse, and waste of government funds.

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 CalHEERS manual override processes. This audit specifically examined the Service Center Division's and Information Technology Division's internal controls during the audit period of January 1, 2023, through December 31, 2023. Our report of this audit is attached.

We appreciate the cooperation and assistance of the Service Center Division's and Information Technology Division's management and staff during our audit. If you have any questions regarding this report, please contact me at (916) 954-3498 or Kirk.Marston@covered.ca.gov.

cc: <u>Executive Office</u>
Jessica Altman, Executive Director
Doug McKeever, Chief Deputy Executive Director, Program
Kathleen Webb, Chief Deputy Executive Director, Operations
Brandon Ross, General Counsel, Program Compliance & Accountability

<u>Service Center Division</u>
Tamara Spears, Deputy Director
Anjonette Dillard, Deputy Director, Consumer Relations & Resolution Branch
Miki Keen, Deputy Director, Operations Branch

<u>Information Technology Division</u>
David Krause, Deputy Chief Information Officer
Tina Mitchell, Chief Information Security Officer

<u>Program Integrity Division</u>
Thien Lam, Director
Kevin Cathy, Branch Chief, Office of Audit Services
Alicia Watts, Section Chief, Office of Audit Services
Kurt Faubion, Audit Manager, Office of Audit Services
Galina Rub, Internal Auditor, Office of Audit Services

REVIEW OF INTERNAL CONTROLS OVER THE CALHEERS MANUAL OVERRIDE PROCESS

COVERED CALIFORNIA
SERVICE CENTER DIVISION
INFORMATION TECHNOLOGY DIVISION

FINAL AUDIT REPORT

ISSUED ON:
MARCH 17, 2025

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

AUDIT TEAM:
KIRK MARSTON, CHIEF AUDIT EXECUTIVE
KEVIN CATHY, BRANCH CHIEF
ALICIA WATTS, SECTION CHIEF
KURT FAUBION, AUDIT MANAGER
GALINA RUB, INTERNAL AUDITOR
RAMEN SINGH, INTERNAL AUDITOR

Table Of Contents

Executive Summary

Objective and Scope

The Office of Audit Services conducted an audit to provide reasonable assurance that internal controls over the CalHEERS manual override process during January 1, 2023, through December 31, 2023, were administered in accordance with policies, procedures, and applicable requirements.

Positive Observations

The following are areas we noted with reasonable assurance where internal controls of the CalHEERS manual override process were identified as effective or strengthened during the audit. The Service Center Division:

- Established a robust set of policies and procedures for performing CalHEERS manual override transactions. Having established policies and procedures minimizes risk and enhances consistency.

- Improved monitoring of employees provisioned with CalHEERS L3 system access, including the development and usage of the "Admin Override Audit Dashboard." This dashboard helps monitor and audit manual overrides, which enhances accountability and integrity of manual override activities.

Reportable Conditions

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

- **Service Center Division L3 system users did not always perform accurate and allowable CalHEERS manual override transactions**

- **Service Center Division did not always provision employees with the correct CalHEERS access levels**

- **Information Technology Division did not ensure quarterly reviews of CalHEERS user accounts were performed**

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

The Service Center Division (SCD) provides comprehensive eligibility and enrollment education and support to Covered California consumers. SCD accomplishes this by responding to consumer inquiries, enrolling consumers in health plans, and promptly resolving challenges that prevent consumers from receiving health and dental benefits.

SCD ensures that their employees have the necessary CalHEERS system capabilities to provide consumers this level of support. Certain situations, such as for appeal adjudications and escalated complex cases, necessitate SCD employees to perform manual override transactions within the CalHEERS system. Examples of these transactions include changing enrollment details, terminating enrollment, and updating enrollment status. As such, SCD ensures that certain employees are provisioned with this manual override capability. These employees are called Level 3 (L3) system users.

Although the Information Technology Division (ITD) oversees the ongoing development and operations of the CalHEERS system, they are not responsible for overseeing actions taken by L3 system users. However, ITD has a role regarding the provisioning and periodic reviews of CalHEERS system access.

Objective

The objective of this audit was to determine whether internal controls over CalHEERS manual override functionalities are in place and operating appropriately.

Scope

The scope of this audit covered the review of the CalHEERS manual override process during the period of January 1, 2023, through December 31, 2023.

Methodology

Our evaluation included gaining an understanding of policies and procedures and testing SCD’s and ITD’s internal controls over the CalHEERS manual override process. Additionally, audit procedures were performed to determine whether SCD management and staff are effectively and efficiently administering CalHEERS manual override processes and provisioning L3 system access in accordance with policies, procedures, and applicable requirements.

Results

Positive Observations

The following are areas we noted with reasonable assurance where internal controls of the CalHEERS manual override process were identified as effective or strengthened during the audit. The Service Center Division:

- Established a robust set of policies and procedures for performing CalHEERS manual override transactions. Having established policies and procedures minimizes risk and enhances consistency.

- Improved monitoring of employees provisioned with CalHEERS L3 system access, including the development and usage of the “Admin Override Audit Dashboard.” This dashboard helps monitor and audit manual overrides, which enhances accountability and integrity of manual override activities.

Finding & Recommendation

Finding #1 – Service Center Division L3 system users did not always perform accurate and allowable CalHEERS manual override transactions

Finding Rating:	Priority	High	Medium	Low

Condition
We reviewed a sample of 80 CalHEERS manual override transactions, and identified that:

- 34 transactions occurred where the L3 system user did not input the corresponding case number from the Salesforce Customer Relationship Management (CRM) system into the "Reasons for Change" section within CalHEERS.
- 2 transactions occurred where the L3 system user did not input the details of what changes were made into the "Note/Description" section within the CRM system.
- 17 transactions were performed by certain L3 system users who did not have the permission levels to perform those transactions based on their positions.

Criteria
Admin Overrides Task Guide SC.625 includes instructions for L3 system users to input corresponding CRM case numbers into the "Reasons for Change" section within CalHEERS.

Priority Support Unit Processing Guide – Documenting in CRM includes instructions for L3 system users to input the details of what changes were made into the "Note/Description" section within the CRM system.

CalHEERS Security Roles Task Guide outlines the policies regarding the appropriate permission levels for L3 system users, based on their respective positions.

Cause
SCD management did not always effectively monitor transactions performed by L3 system users.

Effect
By SCD management not effectively monitoring transactions, there is potential that L3 system users may perform inaccurate or unallowable CalHEERS manual override transactions. This could negatively impact consumers' enrollments, consumers' access to care, SCD operations, and Covered California's reputation.

Recommendation
SCD management should develop formal monitoring procedures to ensure all override transactions are performed accurately and by only allowable L3 system users.

Finding #2 – Service Center Division did not always provision employees with the correct CalHEERS access levels

Finding Rating:	Priority	High	[✓ Medium]	Low

Condition

We reviewed a sample of 40 SCD employees' CalHEERS access levels and identified that:

- 1 employee was provisioned with Level 3 access instead of Level 1.
- 7 employees were provisioned with Level 1 or Level 2 access instead of Level 3.
- 9 employees did not have active system access that should have had active system access.

Criteria

Information Security Policy, Subsection 1055 – Least Privilege, states, in part, "The principle of least privilege is applied to information system processes, roles, and accounts to operate at privilege levels no higher than necessary to accomplish required Exchange/CC missions/business functions."

Cause

SCD employees were not provisioned with the correct level of system access or had inactive system access because:

- Updates to the SCD entitlement catalog were not applied to inactive accounts.
- An employee's access was temporarily elevated for a special project but was not reverted afterward.
- Employees did not actively use their accounts and therefore the account became disabled.

Effect

SCD employees provisioned with a higher level of CalHEERS system access than authorized may result in unauthorized changes to consumer enrollment information. SCD employees provisioned with a lower level of system access than authorized or that do not have active system access may result in the employee not being able to perform their job duties and help consumers when needed.

Recommendation

SCD should work with ITD to ensure accounts are provisioned with the appropriate level of system access and to maintain active system access.

Finding #3 – Information Technology Division did not ensure quarterly reviews of CalHEERS user accounts were performed

Finding Rating:	Priority	High	[✓ Medium]	Low

Condition

We identified that the Information Security Office (ISO) within ITD did not initiate and ensure that quarterly reviews of SCD CalHEERS user accounts were performed to verify that system user access and account privileges were appropriate.

Criteria

Information Security Policy Subsection 1020 – Account Management, states, in part, “All accounts shall be reviewed at least quarterly by the data owner to ensure that access and account privileges are commensurate with job function, need-to-know, and employment status.”

Cause

ITD has not fully implemented a process to ensure SCD CalHEERS user accounts are reviewed at least quarterly.

Effect

If ITD does not ensure SCD is performing quarterly reviews of SCD CalHEERS user accounts, inappropriate access and privileges to CalHEERS may not be identified timely.

Recommendation

ITD should fully implement a process to ensure SCD CalHEERS user accounts are reviewed at least quarterly.

Conclusion

During our audit, SCD implemented several internal control improvements to ensure that only authorized SCD employees are provisioned with L3 access and adhere to SCD CalHEERS manual override policies and procedures. However, as shown in the three findings we identified, opportunities still exist to lower the potential risk of unallowable or inaccurate CalHEERS manual override transactions from occurring. If these findings are not addressed, they could result in negative impacts to consumers' enrollments, consumers' access to care, and helping consumers when needed. In general, the three findings are rated at medium risk levels due to the potential adverse effects to SCD's operations and Covered California as a whole, including potential adverse impact on overall reputation.

Management Response

Presented below is the Service Center Division's and Information Technology Division's management response to the finding which includes their corrective action plans.

Finding 1:	*Service Center Division L3 system users did not always perform accurate and allowable CalHEERS manual override transactions.*
Recommendation 1:	Service Center Division management should develop formal monitoring procedures to ensure all override transactions are performed accurately and by only allowable L3 system users.
SCD Management Response/ Corrective Action Plan	The Service Center will develop formal processes to review and monitor L3 system usage. The Service Center Operations Branch is developing and piloting a formal process to review L3 transactions.
Targeted Completion Date:	July 1, 2025

Finding 2:	*Service Center Division did not always provision employees with the correct CalHEERS access levels.*
Recommendation 2:	Service Center Division should work with ITD to ensure accounts are provisioned with the appropriate level of system access and to maintain active system access.
SCD Management Response/ Corrective Action Plan	The Service Center will partner with ITD to develop processes for reviewing and monitoring CalHEERS provisioning and system access.
Targeted Completion Date:	December 31, 2025

Finding 3:	*Information Technology Division did not ensure quarterly reviews of CalHEERS user accounts were performed.*
Recommendation 3:	Information Technology Division should fully implement a process to ensure SCD CalHEERS user accounts are reviewed at least quarterly.
ITD Management Response/ Corrective Action:	ISO acknowledges that the user account permission reviews were not conducted by ISO. The ISO plans to recruit more staff to assist with manual reviews. ISO is also anticipating the success of the SailPoint Identity project that will provide a platform for a more efficient way to complete assessments.
Targeted Completion Date:	March 31, 2026

Evaluation of Response

The corrective action plans provided by the Service Center Division and 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 and are operating as designed. Additionally, a follow-up audit may be performed to determine the completion and adequacy of the correction action plans.

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

Appendix A

Finding Ratings

Finding	Priority	High	Medium	Low
1. Service Center Division L3 system users did not always perform accurate and allowable CalHEERS manual override transactions			X	
2. Service Center Division did not always provision employees with the correct CalHEERS access levels			X	
3. Information Technology Division did not ensure quarterly reviews of CalHEERS user accounts were performed			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.