



PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT



Information Technology Audit: Health Care Agency Selected Cybersecurity Controls

For the Year Ended July 31, 2021

Audit No. 1943

Report Date: June 30, 2022

Number of Recommendations

0

**Critical Control
Weaknesses**

5

**Significant Control
Weakness**

3

Control Findings

OC Board of Supervisors

CHAIRMAN DOUG CHAFFEE
4th DISTRICT

VICE CHAIRMAN DONALD P. WAGNER
3rd DISTRICT

SUPERVISOR ANDREW DO
1st DISTRICT

SUPERVISOR KATRINA FOLEY
2nd DISTRICT

SUPERVISOR LISA A. BARTLETT
5th DISTRICT



INTERNAL AUDIT DEPARTMENT

Information Technology Audit:
Health Care Agency Selected Cybersecurity Controls

June 30, 2022

AUDIT HIGHLIGHTS

SCOPE OF WORK	Perform an information technology audit of Health Care Agency selected cybersecurity controls for the year ended July 31, 2021.
RESULTS	Content has been removed from this report due to the sensitive nature of the specific findings.
RISKS	Content has been removed from this report due to the sensitive nature of the specific findings.
NUMBER OF RECOMMENDATIONS	Content has been removed from this report due to the sensitive nature of the specific findings.
0	CRITICAL CONTROL WEAKNESSES
5	SIGNIFICANT CONTROL WEAKNESSES
3	CONTROL FINDINGS

Report suspected fraud, or misuse of County resources by vendors, contractors, or County employees to 714.834.3608



INTERNAL AUDIT DEPARTMENT

Audit No. 1943

June 30, 2022

To: Clayton Chau, MD, PhD, MASL
Health Care Agency Director

From: Aggie Alonso, CPA, CIA, CRMA
Internal Audit Department Director

Subject: Information Technology Audit: Health Care Agency Selected Cybersecurity Controls

We have completed an information technology audit of selected cybersecurity controls administered by Health Care Agency for the year ended July 31, 2021. Due to the sensitive nature of specific findings (restricted information), results are redacted from public release. Additional information including background and our objectives, scope, and methodology are included in Appendix A.

HCA concurred with all our recommendations and the Internal Audit Department considers management's response appropriate to the recommendations in this report.

We will include the results of this audit in a future status report submitted quarterly to the Audit Oversight Committee and the Board of Supervisors. In addition, we will request your department complete a Customer Survey of Audit Services, which you will receive shortly after the distribution of our final report.

We appreciate the courtesy extended to us by Health Care Agency personnel during our audit. If you have any questions, please contact me at 714.834.5442 or Assistant Director Scott Suzuki at 714.834.5509.

Attachments

Other recipients of this report:

- Members, Board of Supervisors
- Members, Audit Oversight Committee
- CEO Distribution
- HCA Distribution
- Foreperson, Grand Jury
- Robin Stieler, Clerk of the Board
- Eide Bailly LLP, County External Auditor

INTERNAL AUDIT DEPARTMENT

RESULTS

Content has been removed from this report due to the sensitive nature of the specific findings.

AUDIT TEAM	Scott Suzuki, CPA, CIA, CISA, CFE Jimmy Nguyen, CISA, CFE, CEH Scott Kim, CPA, CISA, CFE Stephany Pantigoso Mari Elias, DPA	Assistant Director IT Audit Manager II IT Audit Manager I Senior Internal Auditor Administrative Services Manager
-------------------	---	---



INTERNAL AUDIT DEPARTMENT

APPENDIX A: ADDITIONAL INFORMATION

OBJECTIVES	<p>Our audit objectives were to determine if Health Care Agency IT controls provide reasonable assurance:</p> <ol style="list-style-type: none"> 1. Controls for assets ensure the installation, spread, and execution of malicious applications, code, or scripts are prevented. 2. Controls for applications ensure only authorized applications can operate, vulnerabilities are managed, and any changes to critical systems are authorized. 3. Controls for users to ensure accounts are properly managed and access is authorized. 4. Controls for network to help detect and recover from an attack.
SCOPE & METHODOLOGY	<p>Our audit scope was limited to select high-risk cybersecurity controls at Health Care Agency for the year ended July 31, 2021. Our methodology included inquiry, observation, examination of documentation, and sampling of relevant items.</p>
EXCLUSIONS	<p>We did not examine application controls or any processes that involve external parties such as OCIT or systems managed by the State of California, nor any services/activities performed or provided by the County or state’s third-party vendors.</p>
PRIOR AUDIT COVERAGE	<p>No audits of this scope have been issued by Internal Audit for Health Care Agency in the last 10 years.</p>
BACKGROUND	<p>The Health Care Agency is a regional provider, charged with protecting and promoting individual, family, and community health through coordination of public and private sector resources. HCA’s service environment is complex, with 180 different funding sources and over 200 state and federal mandates. The mandates under which HCA operates require the County to provide for, or to regulate, certain health services. Many also carry specific requirements for staffing, operations, claiming and record-keeping.</p> <p>HCA is composed of the following service areas:</p> <ul style="list-style-type: none"> • Correctional Health Services • Director’s Office • Finance & Administrative Services • Medical Health Services • Mental Health & Recovery Services • Public Health Services • Strategy & Special Services



INTERNAL AUDIT DEPARTMENT

<p>PURPOSE & AUTHORITY</p>	<p>We performed this audit in accordance with the FY 2021-22 Audit Plan and Risk Assessment approved by the Audit Oversight Committee (AOC) and the Board of Supervisors (Board).</p>
<p>FOLLOW-UP PROCESS</p>	<p>In accordance with professional standards, the Internal Audit Department has a process to follow-up on its recommendations. A first follow-up audit will generally begin six months after release of the initial report.</p> <p>The AOC and Board expect that audit recommendations will typically be implemented within six months or sooner for significant and higher risk issues. A second follow-up audit will generally begin six months after release of the first follow-up audit report, by which time all audit recommendations are expected to be implemented. Any audit recommendations not implemented after the second follow-up audit will be brought to the attention of the AOC at its next scheduled meeting.</p> <p>A Follow-Up Audit Report Form is attached and is required to be returned to the Internal Audit Department approximately six months from the date of this report in order to facilitate the follow-up audit process.</p>
<p>MANAGEMENT'S RESPONSIBILITY FOR INTERNAL CONTROL</p>	<p>In accordance with the Auditor-Controller's County Accounting Manual No. S-2 Internal Control Systems: "All County departments/agencies shall maintain effective internal control systems as an integral part of their management practices. This is because management has primary responsibility for establishing and maintaining the internal control system. All levels of management must be involved in assessing and strengthening internal controls." Internal control should be continuously evaluated by management and weaknesses, when detected, must be promptly corrected. The criteria for evaluating internal control is the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control – Integrated Framework. Our audit complements but does not substitute for department management's continuing emphasis on control activities and monitoring of control risks.</p>
<p>INTERNAL CONTROL LIMITATIONS</p>	<p>Because of inherent limitations in any system of internal control, errors or irregularities may nevertheless occur and not be detected. Specific examples of limitations include, but are not limited to, resource constraints, unintentional errors, management override, circumvention by collusion, and poor judgment. Also, projection of any evaluation of the system to future periods is subject to the risk that procedures may become inadequate because of changes in conditions or the degree of compliance with the procedures may deteriorate. Accordingly, our audit would not necessarily disclose all weaknesses in the department's operating procedures, accounting practices, and compliance with County policy.</p>



INTERNAL AUDIT DEPARTMENT

APPENDIX B: REPORT ITEM CLASSIFICATION

Critical Control Weakness	Significant Control Weakness	Control Finding
<p>These are audit findings or a combination of audit findings that represent critical exceptions to the audit objective(s) and/or business goals. Such conditions may involve either actual or potential large dollar errors or be of such a nature as to compromise the department's or County's reputation for integrity. Management is expected to address Critical Control Weaknesses brought to its attention immediately.</p>	<p>These are audit findings or a combination of audit findings that represent a significant deficiency in the design or operation of internal controls. Significant Control Weaknesses require prompt corrective actions.</p>	<p>These are audit findings concerning the effectiveness of internal control, compliance issues, or efficiency issues that require management's corrective action to implement or enhance processes and internal control. Control Findings are expected to be addressed within our follow-up process of six months, but no later than twelve months.</p>



INTERNAL AUDIT DEPARTMENT

APPENDIX C: HEALTH CARE AGENCY MANAGEMENT RESPONSE

Content has been removed from this report due to the sensitive nature of the specific findings.

