



PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT



Information Technology Audit: CAPS+ Application Security Controls

For the period July 1, 2022
through June 30, 2023

Audit No. 2311 (2046)
Report Date: June 28, 2024

Number of Recommendations

0

Critical Control Weaknesses

0

Significant Control Weaknesses

4

Control Findings

OC Board of Supervisors

CHAIRMAN DONALD P. WAGNER
3rd DISTRICT

VICE CHAIRMAN DOUG CHAFFEE
4th DISTRICT

SUPERVISOR ANDREW DO
1st DISTRICT

SUPERVISOR VICENTE SARMIENTO
2nd DISTRICT

SUPERVISOR KATRINA FOLEY
5th DISTRICT



INTERNAL AUDIT DEPARTMENT

Information Technology Audit:
CAPS+ Application Security Controls
June 28, 2024

AUDIT HIGHLIGHTS

SCOPE OF WORK	Perform an information technology audit of CAPS+ Financial System (FS) Application Security Controls administered or monitored by the Auditor-Controller (A-C) for the period July 1, 2022 to June 30, 2023.
RESULTS	Content has been removed from this report due to the sensitive nature of the specific findings.
RISKS IDENTIFIED	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
0	SIGNIFICANT CONTROL WEAKNESSES
4	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. 2311 (2046)

June 28, 2024

To: Andrew N. Hamilton, CPA
Auditor-Controller

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

Subject: Information Technology Audit: CAPS+ Application Security Controls

We have completed an information technology audit of CAPS+ Financial System (FS) Application Security Controls administered or monitored by the Auditor-Controller (A-C) for the period July 1, 2022 through June 30, 2023. 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.

A-C 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 A-C during our audit. If you have any questions, please contact me at (714) 834-5442 or Senior IT Audit Manager Jimmy Nguyen at (714) 834-2526.

Attachments

Other recipients of this report:

- Members, Board of Supervisors
- Members, Audit Oversight Committee
- County Executive Office Distribution
- Auditor-Controller 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 Results due to the sensitive nature of the specific findings.

AUDIT TEAM	Jimmy Nguyen, CISA, CFE, CEH Stephany Franco Thuy Luu	Senior IT Audit Manager Senior Auditor Staff Specialist
-------------------	---	---



INTERNAL AUDIT DEPARTMENT

APPENDIX A: ADDITIONAL INFORMATION

<p>OBJECTIVES</p>	<p>Our audit objectives were to evaluate A-C’s design, implementation, and operating effectiveness of IT and application controls over CAPS+ to determine if IT control activities for:</p> <ol style="list-style-type: none"> 1. Account management and access control management provide reasonable assurance of proper user and privileged account administration. 2. Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they impact the enterprise. 3. Data recovery capabilities provide reasonable assurance enterprise assets can be restored to a pre-incident and trusted state.
<p>SCOPE & METHODOLOGY</p>	<p>Our audit scope was limited to A-C selected CAPS+ cybersecurity controls for the period July 1, 2022 to June 30, 2023. Our methodology included inquiry, observation, examination of documentation, and sampling of relevant items.</p>
<p>EXCLUSIONS</p>	<p>We did not examine application controls or any processes that involve external parties nor any services/activities performed or provided by the County of Orange’s third-party vendors.</p>
<p>PRIOR AUDIT COVERAGE</p>	<p>An audit with a similar scope, Information Technology Audit: A-C Information Technology General Controls, Audit No. 1741, was issued on March 6, 2019.</p>



INTERNAL AUDIT DEPARTMENT

BACKGROUND

The Auditor-Controller's mission is to promote public oversight, provide accountability, and support financial decision-making for the County of Orange. The Auditor-Controller's vision is to be the county's trusted source of financial information to account for the past, direct the present, and shape the future. As the Auditor-Controller's Office carries out its vision and mission, it will conduct business with the highest ethical and due diligence standards and demonstrate commitment to the citizens of the county, other county departments, special districts, and its own employees. The Auditor-Controller provides accounting support services to eight county departments, prepares the Annual Comprehensive Financial Report (ACFR), prepares the Countywide Cost Allocation Plan (CWCAP), oversees the Countywide Accounting and Personnel System (CAPS+) which records and tracks financial and human resource transactions for the county and administers the County Property Tax System (PTS).

The Auditor-Controller's Office is comprised of five divisions: Central Accounting Operations, Satellite Operations, Information Technology, Executive and Administration, and Internal Audit. This audit worked with the Information Technology division.

The Information Technology (IT) division is comprised of Project Management and Security Services, Network and Desktop Support, and Functional and Technical Support. The Project Management team supports a variety of IT projects and takes the lead in certain system upgrade and development efforts to increase County efficiency. The Security Services team oversees the issuance and safeguarding of the controlled assets for the Auditor-Controller's Office, the enforcement of IT policies and procedures, and the development of security standards. The Server and Desktop Support team provides operational and desktop support to systems' servers and Auditor-Controller staff. The CAPS+ Functional and Technical Support team keeps the Auditor-Controller and Countywide financial systems running accurately and timely. The support enables the Auditor-Controller's Office and financial professionals throughout the County to run systems and access the information necessary to perform their jobs and to meet their obligations.

Some of the systems supported by the division include the county-wide CAPS+ Financial and Procurement and CAPS+ Human Resource and Payroll Systems, CAPS+ System Security & Workflow administration, document imaging and management system (ERMI), Financial and Procurement Data Warehouse, and property tax systems. These systems are a vital component of the County's infrastructure and are required for County operations, such as financial planning, budget development, maintaining financial records, generating financial statements, collecting costs for federal and state program billings, procuring goods and services, making vendor and trust disbursements, processing the County's payroll, and administering personnel records.



INTERNAL AUDIT DEPARTMENT

PURPOSE & AUTHORITY	We performed this audit in accordance with the FY 2023-24 Audit Plan and Risk Assessment approved by the Audit Oversight Committee (AOC) and the Board of Supervisors (Board).
PROFESSIONAL STANDARDS	Our audit was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing issued by the International Internal Audit Standards Board.
FOLLOW-UP PROCESS	<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>
MANAGEMENT'S RESPONSIBILITY FOR INTERNAL CONTROL	In accordance with the A-C'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.



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: AUDITOR-CONTROLLER MANAGEMENT RESPONSE

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

