INTERNAL AUDIT DEPARTMENT

Information Technology Audit:
OC District Attorney
Selected Cybersecurity Controls
For the Year Ended June 30, 2025

Audit No. 2412
Report Date: January 28, 2026

Number of Recommendations

0	Critical Control Weaknesses
0	Significant Control Weaknesses
3	Control Findings

INTERNAL AUDIT DEPARTMENT

District Attorney-Public Administrator Selected Cybersecurity Controls
January 28, 2026

AUDIT HIGHLIGHTS

SCOPE OF WORK	Perform an audit of District Attorney-Public Administrator's (OCDA) selected cybersecurity controls to determine whether OCDA strengthened its cybersecurity resilience since its 2023 cyber incident to provide reasonable assurance in reducing the risk of future cyberattacks and to determine whether selected controls over a critical OCDA-managed system ensure sensitive data is restricted, and that account access and system changes are properly managed for the year ended June 30, 2025.
RESULTS	We concluded that OCDA strengthened its cybersecurity resilience since their cyber incident in 2023. In addition, OCDA's critical system controls provide reasonable assurance that sensitive data is restricted, and account access and system changes are properly managed in compliance with best practices. However, we noted certain areas where controls could be enhanced.
RISKS	As a result of our findings, potential risks include: • Unauthorized access or inappropriate changes to sensitive case data in a critical OCDA-managed case information system. • Risk of unauthorized or improperly tested changes being introduced into the production environment, which can lead to system down time. • Limited awareness and understanding of information technology (IT) business processes and controls established by management, which could result in misuse of IT resources and potential cybersecurity violations.
NUMBER OF RECOMMENDATIONS 0 CRITICAL CONTROL WEAKNESSES 0 SIGNIFICANT CONTROL WEAKNESSES 3 CONTROL FINDINGS	Opportunities for enhancing internal controls include: • Enhancing documentation of user access reviews performed, strengthening the review process to include existing user accounts, and ensuring timely notification to OCDA IT of employee role changes to disable access to a critical system timely. • Ensuring documentation is retained to provide evidence and assurance that critical system changes are properly documented, tested, and approved before deployment into production. • Finalizing IT policies and procedures for Data Protection, Change Management, Account Management and Vulnerability Management.

Report suspected fraud, or misuse of County resources by vendors, contractors, or County employees to (714) 834-3608

INTERNAL AUDIT DEPARTMENT

Audit No. 2412

January 28, 2026

To: Todd Spitzer
District Attorney-Public Administrator

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

Digitally signed by Agripino Alonso
Date: 2026.01.28 13:51:40 -08'00'

Subject: District Attorney-Public Administrator Selected Cybersecurity Controls

We have completed an audit of District Attorney-Public Administrator (OCDA) Selected Cybersecurity Controls administered by OCDA for the year ended June 30, 2025. Details of our results and recommendations immediately follow this letter. Additional information including background, and our objectives, scope, and methodology are included in Appendix A.

The District Attorney-Public Administrator 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 OCDA during our audit. If you have any questions, please contact me at (714) 834-5442 or Deputy Director Jose Olivo at (714) 834-5509.

Attachments

Other recipients of this report:
Members, Board of Supervisors
Members, Audit Oversight Committee
County Executive Office Distribution
OCDA Distribution
Foreperson, Grand Jury
Robin Stieler, Clerk of the Board
Eide Bailly LLP, County External Auditor

RESULTS	
BUSINESS PROCESS & INTERNAL CONTROL STRENGTHS	Business process and internal control strengths that were developed as a result of the recent cyber incident that occurred in 2023 include: ✓ OCDA implemented multiple information technology (IT) infrastructure security control improvements, including managed detection and response, enhanced monitoring and visibility, network architecture redesign, 24/7 threat detection and response, business continuity, and disaster recovery. ✓ OCDA deployed a modern security solution to enhance logging and threat detection capabilities. ✓ OCDA deployed a modernized cloud-based cybersecurity platform for endpoint protection, across all system devices connected to the network domain. ✓ OCDA subscribes to the County's SOC (security operations center) for after-hours, weekend, and holiday coverage to ensure 24/7 monitoring and response of abnormal activity on its network. ✓ OCDA utilizes a security cloud platform for security and compliance with government cloud storage requirements. ✓ OCDA maintains an updated incident response plan (BCDR), developed and tested in collaboration with Orange County Information Technology (OCIT) and Science Application International Corporation. ✓ OCDA has a data inventory list for a critical system.

FINDING NO. 1	**CMS User Account Management** Departments need to perform user access reviews (UAR) over critical systems to ensure account profiles are appropriate for user's job duties. While OCDA performs UARs, their review is limited and inconsistent. Specifically, OCDA: • Only performs UARs for staff that have been terminated or transferred from OCDA to ensure their access has been removed. As a result, they do not review all system users, including active OCDA employees that may have changed job responsibilities, to ensure access permissions are necessary and appropriate based on their current roles and responsibilities. • Does not centralize UAR documentation and the documentation does not clearly show what was reviewed and approved. We also noted, OCDA does not have a formalized process, including timeframe requirements, for when the business manager must notify IT of employee role changes that require updated access permissions. While our review of OCDA's user list did not identify any instances of inappropriate access, OCDA should strengthen their processes to ensure account profiles are appropriate for user's job duties.
CATEGORY	**Control Finding**
RISK	Incomplete UARs reduce accountability and may lead to unauthorized access or inappropriate changes to sensitive case data in a critical OCDA-managed case information system. Untimely notification of employee role change could lead to unauthorized access.
RECOMMENDATION	OCDA management: A. Strengthen their UAR process to include the review of all existing user accounts to ensure access is restricted to personnel with a direct business need. B. Improve documentation for completion of UARs to clearly show what was reviewed and approved. C. Establish a process, including timeframe requirements, to notify OCDA IT of employee role changes and update access rights in critical systems, timely.
MANAGEMENT RESPONSE	**Concur**. We will strengthen our documentation process by centralizing UAR records to clearly reflect reviews and approvals. Additionally, we will work with HR to reestablish a consistent cadence for office move notifications and role changes to ensure timely updates to access rights.

FINDING NO. 2	**CMS Change Management Documentation** Departments need to ensure critical system changes are properly documented, tested, and approved before deployment into production. Documentation should be retained to clearly show who requested, tested, approved, and deployed the change. During the audit, OCDA demonstrated [redacted] process within [redacted] which a system change request begins with completing a [redacted] form and continues through email-based coordination to [redacted] for execution. This workflow supports the full lifecycle from request to deployment. However, documentation related to change requests, testing, and approvals performed by separate staff and tracked via email was not formally centralized. As a result, it was difficult to readily provide assurance that all steps were consistently followed. OCDA should retain documentation in a centralized location to support change management controls. Centralizing change management documentation could be enhanced using application change control software.
CATEGORY	**Control Finding**
RISK	The lack of centralized change management documentation for critical systems increases the risk of unauthorized, or improperly tested changes being introduced into the production environment, which can lead to system downtime.
RECOMMENDATION	OCDA management retain documentation to provide evidence and assurance that critical system changes are properly documented, tested, and approved before deployment into production.
MANAGEMENT RESPONSE	**Concur**. We will explore opportunities to improve our change management process by centralizing documentation within [redacted] to ensure visibility and consistency. Additionally, we will review ways to enhance documentation practices to clearly capture requests, testing, approvals, and deployments.

FINDING NO. 3	**Draft IT Policies and Procedures** Departments need documented IT policies and procedures that outline specific steps for performing tasks to ensure consistency and accuracy. They act as a guide for employees, providing clear instructions and best practices for completing tasks. While OCDA has processes in place to perform daily business operations and multiple IT policies and procedures in draft form, OCDA does not have finalized IT policies or procedures for Data Protection, Change Management, Account Management and Vulnerability Management.
CATEGORY	**Control Finding**
RISK	Without formal IT policies and procedures, there can be limited awareness and understanding of IT business processes and controls established by management, which could result in misuse of IT resources and potential cybersecurity violations.
RECOMMENDATION	OCDA management finalize IT policies and procedures for Data Protection, Change Management, Account Management & Vulnerability Management, to help ensure consistency and accuracy in the work staff perform.
MANAGEMENT RESPONSE	**Concur**. We will begin reviewing and developing these policies and procedures in coordination with OCDA IT governance teams to ensure alignment and consistency across key areas.

AUDIT TEAM	Michael Dean, CPA, CIA, CISA	Assistant Deputy Director
	Jimmy Nguyen, CISA, CFE, CEH	Senior IT Audit Manager
	Michael Steinhaus, CISA, CIA, CPA	IT Audit Manager
	JC Lim, CIA, CISA, CFE	Senior IT Auditor
	Gabriela Cabrera, CIA	Administrative Services Manager

APPENDIX A: ADDITIONAL INFORMATION

OBJECTIVES	A. Determine whether OCDA strengthened its cybersecurity resilience since its 2023 cyber incident to provide reasonable assurance in reducing the risk of future cyberattacks. B. Evaluate the effectiveness of selected internal controls over a critical OCDA-managed system to determine whether sensitive data is restricted, and whether account access and system changes are properly managed in compliance with best practices.
SCOPE & METHODOLOGY	Our engagement scope was limited to OCDA's cybersecurity improvements and selected internal controls over a critical OCDA-managed case information system for the year ended June 30, 2025. Our methodology included inquiry, observation, examination of documentation, and sampling of relevant items.
EXCLUSIONS	We did not evaluate application controls or processes that involve external parties such as OCIT, the State of California, or third-party vendors.
PRIOR AUDIT COVERAGE	We issued our most recent OCDA cybersecurity audit report (Audit No. 2041) on September 24, 2021.
BACKGROUND	The mission of the OCDA is to enhance public safety and welfare, to protect and respect crime victims, and to create security in the community through the vigorous enforcement of criminal and civil laws in a just, honest, efficient, and ethical manner. The OCDA IT division, which is separate from OCIT, provides secure, reliable, and innovative technology solutions that empower the OCDA to pursue justice effectively. The IT division supports prosecutors, investigators, and staff with systems that ensure data integrity, streamline operations, and enhance public safety through strategic IT services. OCDA was the victim of a cyberattack on October 20, 2023. As a result, OCDA immediately shut down and isolated its IT systems to prevent further intrusion. OCDA worked with the FBI, cybersecurity experts, and OCIT to investigate the breach and ensured the continued functionality of the criminal justice system. OCDA uses an in-house developed critical system which tracks all active and closed cases.

PURPOSE & AUTHORITY	We performed this audit in accordance with the Fiscal Year 2024-25 Audit Plan and Risk Assessment approved by the Board of Supervisors (Board).
PROFESSIONAL STANDARDS	Our audit was conducted in conformance with the Global Internal Audit Standards issued by the International Internal Audit Standards Board.
FOLLOW-UP PROCESS	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 the release of the initial report. The Audit Oversight Committee (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 the 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. 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 to facilitate the follow-up audit process.
MANAGEMENT'S RESPONSIBILITY FOR INTERNAL CONTROL	In accordance with the Auditor-Controller's County Accounting Manual No. S-2 Internal Control Systems: "All County departments shall establish effective internal controls as department management is responsible for internal control. Department management shall also continuously assess and strengthen internal control by evaluating internal control systems and promptly correcting weaknesses when detected." The criterion for evaluating internal control is the Committee of Sponsoring Organizations of the Treadway Commission Internal Control – Integrated Framework: 2013. Our audit complements but does not substitute for department management's continuing emphasis on control activities and monitoring of control risks.
INTERNAL CONTROL LIMITATIONS	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.

APPENDIX B: REPORT ITEM CLASSIFICATION

Critical Control Weakness	Significant Control Weakness	Control Finding
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.	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.	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.

APPENDIX C: OCDA MANAGEMENT RESPONSE

OFFICE OF THE
DISTRICT ATTORNEY
ORANGE COUNTY, CALIFORNIA
TODD SPITZER

January 16, 2026

Aggie Alonso, CPA, CIA, CRMA
Internal Audit Department Director
Orange County Internal Audit Department
601 N. Ross St., 5th Floor
Santa Ana, CA, 92701

RE: District Attorney-Public Administrator Selected Cybersecurity Controls (Audit No. 2412)

Dear Director Alonso:

This letter is in response to the District Attorney-Public Administrator Selected Cybersecurity Controls (Audit No. 2412).

Finding No. 1 CMS User Account Management

Recommendation No. 1:

A. Strengthen their UAR process to include the review of all existing user accounts to ensure access is restricted to personnel with a direct business need.

B. Improve documentation for completion of UARs to clearly show what was reviewed and approved.

C. Establish a process, including timeframe requirements, to notify OCDA IT of employee role changes and update access rights in critical systems, timely.

OCDA Management Response: Concur. We will strengthen our documentation process by centralizing UAR records to clearly reflect reviews and approvals. Additionally, we will work with HR to reestablish a consistent cadence for office move notifications and role changes to ensure timely updates to access rights.

☒ MAIN OFFICE
300 N. FLOWER ST.
SANTA ANA, CA 92703
(714) 834-3600

☐ NORTH OFFICE
1275 N. BERKELEY AVE.
FULLERTON, CA 92832
(714) 773-4480

☐ WEST OFFICE
8141 13TH STREET
WESTMINSTER, CA 92683
(714) 896-7261

☐ HARBOR OFFICE
4601 JAMBOREE RD.
NEWPORT BEACH, CA 92660
(949) 476-4650

☐ JUVENILE OFFICE
341 CITY DRIVE SOUTH
ORANGE, CA 92868
(714) 935-7624

☐ CENTRAL OFFICE
700 CIVIC CENTER DR. W.
SANTA ANA, CA 92701
(714) 834-3552

Finding No. 2 CMS Change Management Documentation

Recommendation No. 2: OCDA management retains documentation to provide evidence and assurance that critical system changes are properly documented, tested, and approved before deployment into production.

OCDA Management Response: Concur. We will explore opportunities to improve our change management process by centralizing documentation within [redacted] to ensure visibility and consistency. Additionally, we will review ways to enhance documentation practices to clearly capture requests, testing, approvals, and deployments.

Finding No. 3 Draft IT Policies and Procedures

Recommendation No. 3: OCDA management finalizes IT policies and procedures for Data Protection, Change Management, Account Management & Vulnerability Management, to help ensure consistency and accuracy in the work staff perform.

OCDA Management Response: Concur. We will begin reviewing and developing these policies and procedures in coordination with the OCDA IT governance team to ensure alignment and consistency across key areas.

I would like to take the opportunity to thank you and your staff for the courtesy and professionalism that they displayed during the audit. If you have any questions regarding our response, please contact Chief Information Officer Ed Lee at 714-347-8768.

Sincerely,

Todd Spitzer
District Attorney