PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

Information Technology Audit: District Attorney-Public Administrator Selected Cybersecurity Controls

For the Year Ended July 31, 2020

Audit No. 2041
Report Date: September 24, 2021

Number of Recommendations

3	Critical Control Weaknesses
5	Significant Control Weaknesses
3	Control Findings

OC Board of Supervisors

CHAIRMAN ANDREW DO	VICE CHAIRMAN DOUG CHAFFEE	SUPERVISOR KATRINA FOLEY	SUPERVISOR DONALD P. WAGNER	SUPERVISOR LISA A. BARTLETT
1st DISTRICT	4th DISTRICT	2nd DISTRICT	3rd DISTRICT	5th DISTRICT

PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

Information Technology Audit:
District Attorney-Public Administrator Selected Cybersecurity Controls

September 24, 2021

AUDIT HIGHLIGHTS

SCOPE OF WORK	Perform an Information Technology Audit of District Attorney-Public Administrator (OCDA) selected cybersecurity controls for the year ended July 31, 2020.
RESULTS	We concluded: • Password controls for critical systems should be improved. • Controls to prevent unauthorized access should be improved. • Controls over inventory and controls of hardware assets were generally effective. • Controls over vulnerability management should be improved. • Controls over malware defense should be improved. • Controls over data recovery capabilities should be improved.
RISKS	As a result of our findings, potential risks include: • Unauthorized logical access to, and exposure of, sensitive data. • Known vulnerabilities not patched could be exploited by threat actors to gain unauthorized access and perform malicious actions. • Installation, spread, and execution of malicious code that could result in a cybersecurity incident such as data exposure and unauthorized access. • Incomplete backup data or data cannot be restored successfully when needed.
NUMBER OF RECOMMENDATIONS 3 CRITICAL CONTROL WEAKNESSES 5 SIGNIFICANT CONTROL WEAKNESSES 3 CONTROL FINDINGS	Opportunities for enhancing internal control include: • Ensuring password configuration settings conform to best practices. • Performing periodic certification reviews of privileged system/service accounts and user access. • Implementing a central log management system. • Ensuring critical web application connectivity is secured. • Ensuring all network systems have most current security updates and anti-malware installed. • Ensuring backups are periodically tested for completeness and off-site backup media management tool is limited to appropriate personnel.

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

AUDIT NO. 2041

PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

Audit No. 2041

September 24, 2021

To: Todd Spitzer
District Attorney-Public Administrator

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

Subject: Information Technology Audit: District Attorney-Public Administrator Selected Cybersecurity Controls

---

We have completed an Information Technology Audit of District Attorney-Public Administrator (OCDA) selected cybersecurity controls for the year ended July 31, 2020. Due to the sensitive nature of specific findings (restricted information), only the result for Finding No. 10 immediately follows this letter. Results for the remaining findings are included in Appendix A (which is redacted from public release) and additional information including background and our objectives, scope, and methodology are included in Appendix B.

OCDA 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 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
District Attorney-Public Administrator Distribution
Foreperson, Grand Jury
Robin Stieler, Clerk of the Board of Supervisors
Eide Bailly LLP, County External Auditor

RESULTS

BUSINESS PROCESS & INTERNAL CONTROL STRENGTHS	Business process and internal control strengths noted during our audit include: ✓ Robust data backup and recovery software is used to ensure continuous data availability for critical systems. ✓ Comprehensive IT asset management software is used to track and ensure that only authorized systems are connected to the network. ✓ Department end users do not have privileged access to their workstations. ✓ Workstations must be installed with a unique digital certificate in order to be connected to the department network domain. ✓ Remote users must use Virtual Private Network (VPN) in order to securely connect to the department network.

FINDING NOS. 1 - 9	Removed due to the sensitive nature of the findings.

FINDING NO. 10	**Department IT Policy & Procedures** Departmental IT policy and procedures were in various stages of development. OCDA IT has developed draft revisions to some key policy and procedures (e.g., privileged user access rights management, provisioning of new user access, deprovision user access upon separation, vulnerability management, IT inventory of asset, malware software), but has not developed a policy and procedure for disaster recovery testing. Cybersecurity incidents are becoming more common. Accordingly, to properly prepare and increase the opportunity for a department to understand, manage, and recover from a cybersecurity incident, customized procedures, including data collection, team responsibilities, legal procedures, and communication strategies are important to have on-hand and documented.
CATEGORY	**Control Finding**
RISK	Lack of IT policy and procedures can result in a lack of understanding of IT business processes, cybersecurity violations, delayed implementation of systems, or delayed response to a cybersecurity incident.

RECOMMENDATION	OCDA management finalize comprehensive IT policy and procedures that govern all critical IT business processes.
MANAGEMENT RESPONSE	**Concur**. DA Management to finalize draft documents on IT policy and procedures. Existing IT policies and procedures were traditionally maintained by the IT Division Head. IT will refine the existing policy and submit to the Department Head for review and approval.

FINDING NO. 11	Removed due to the sensitive nature of the finding.

AUDIT TEAM	Scott Suzuki, CPA, CIA, CISA, CFE	Assistant Director
	Jimmy Nguyen, CISA, CFE, CEH	IT Audit Manager II
	Scott Kim, CPA, CISA, CFE	IT Audit Manager I
	Zan Zaman, CPA, CIA, CISA	Audit Manager
	Mari Elias, DPA	Administrative Services Manager

APPENDIX A: RESTRICTED INFORMATION

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

APPENDIX B: ADDITIONAL INFORMATION

OBJECTIVES	Our audit objectives were to determine if OCDA selected cybersecurity controls: 1. Are configured to reduce the risk of unauthorized access to critical systems. 2. Provide reasonable assurance access controls over critical systems are appropriate to ensure access is limited to authorized individuals. 3. Provide reasonable assurance controls over inventory and controls of hardware assets are appropriate to ensure inventory of assets is performed and only authorized systems are connected to the network. 4. Provide reasonable assurance controls over continuous vulnerability management are appropriate to ensure vulnerabilities are managed to identify, remediate, and minimize the window of opportunity for attackers. 5. Provide reasonable assurance controls over malware defense are appropriate to ensure protection from installation, spread, and execution of malicious code at multiple points. 6. Provide reasonable assurance controls over data recovery capabilities are appropriate to ensure that critical data backups are complete and data can be recovered in an emergency.
SCOPE & METHODOLOGY	Our audit scope was limited to high-risk cybersecurity controls over governance, security management, and computer operations at OCDA for the year ended July 31, 2020. Our methodology included inquiry, observation, examination of documentation, and sampling of relevant items.
EXCLUSIONS	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.
PRIOR AUDIT COVERAGE	An audit with similar scope, Information Technology Audit: OCDA Computer General Controls: Audit No. 1143, was issued on April 29, 2013.
BACKGROUND	The Office of the Orange County District Attorney's mission is to enhance public safety and welfare and 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. OCDA IT supports and manages the department's network infrastructure security and critical systems.

INTERNAL AUDIT DEPARTMENT

PURPOSE & AUTHORITY	We performed this audit in accordance with the FY 2020-21 Audit Plan and Risk Assessment approved by the Audit Oversight Committee (AOC) and the Board of Supervisors (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 release of the initial report. 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. 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.
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/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 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 C: 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 D: OCDA MANAGEMENT RESPONSE

Content in Appendix D has been removed from this report due to the sensitive nature of the management response.