PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

Information Technology Audit: Clerk-Recorder Selected Cybersecurity Controls

For The Period July 1, 2022 To May 31, 2023

Audit No. 2151
Report Date: September 28, 2023

Number of Recommendations

0	Critical Control Weaknesses
4	Significant Control Weaknesses
2	Control Findings

OC Board of Supervisors

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

PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

Information Technology Audit:
Clerk-Recorder Selected Cybersecurity Controls

September 28, 2023

AUDIT HIGHLIGHTS

SCOPE OF WORK	Perform an information technology audit of Clerk-Recorder selected cybersecurity controls for the period July 1, 2022 to May 31, 2023.
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	
4 SIGNIFICANT CONTROL WEAKNESSES	
2 CONTROL FINDINGS	

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

PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

Audit No. 2151

September 28, 2023

To: Hugh Nguyen
Clerk-Recorder

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

Digitally signed by Agripino Alonso
Date: 2023.09.28 14:43:32 -07'00'

Subject: Information Technology Audit: Clerk-Recorder Selected Cybersecurity Controls

---

We have completed an information technology audit of selected cybersecurity controls administered by Clerk-Recorder for the period July 1, 2022 to May 31,2023. 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.

Clerk-Recorder 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 Clerk-Recorder personnel during our audit. If you have any questions, please contact me at (714) 834-5442 or 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 Officer Distribution
Clerk Recorder Distribution
Foreperson, Grand Jury
Robin Stieler, Clerk of the Board
Eide Bailly LLP, County External Auditor

PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

RESULTS

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

AUDIT TEAM	Jimmy Nguyen, CISA, CFE, CEH	IT Audit Manager II
	Zan Zaman, CPA, CIA, CISA	IT Audit Manager I
	Thuy Luu	Staff Specialist

APPENDIX A: ADDITIONAL INFORMATION

OBJECTIVES	Our audit objectives were to evaluate Clerk-Recorder's design, implementation, and operating effectiveness of internal control to determine if IT control activities for: 1. Account management and access control management provide reasonable assurance of proper user and privileged account administration. 2. Vulnerability management provide reasonable assurance the opportunity for attack is reduced. 3. Data recovery capabilities controls provide reasonable assurance enterprise assets can be restored to a pre-incident and trusted state.
SCOPE & METHODOLOGY	Our audit scope was limited to select high-risk cybersecurity controls at Clerk-Recorder for the period July 1, 2022 to May 31, 2023. Our methodology included inquiry, observation, examination of documentation, and sampling of relevant items.
EXCLUSIONS	We did not examine Clerk-Recorder's non-IT business process.
PRIOR AUDIT COVERAGE	An audit with similar scope, Clerk-Recorder County Agency Vital Records Index Access System, Audit No. 1840, was issued on March 22, 2019.

BACKGROUND	The Clerk-Recorder's mission is to maintain a safe and secure repository for public records; and to provide cost effective platforms to easily access records, while safeguarding the confidentiality of personal information. Clerk-Recorder is comprised of six divisions: (1) Administrative Services, (2) Recorder Operations, (3) Clerk Operations, (4) Information Systems, (5) Financial Services, and (6) Archives. The primary purpose of the Clerk-Recorder Information Systems department is to: 1. Ensure a cost-effective manner and use of automated processes and digital image technology to make it easier for the public and business community to access our records. 2. Manage and support the technology infrastructure and systems used by the department. 3. Ensuring the department's computer network, systems are reliable, efficient and secure from digital attacks. 4. Installing, configuring, and maintaining the organization's computer systems, including servers, workstations, and applications. 5. Ensuring the organization's data and records are backed up, secured, and available for authorized users. 6. Providing technical assistance and troubleshooting for users and patrons who encounter problems with their technology tools. 7. Developing and maintaining small-scale software applications that are specific to the department's needs.

PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

PURPOSE & AUTHORITY	We performed this audit in accordance with the FY 2022-23 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	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.

PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

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.

PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

APPENDIX C: CLERK-RECORDER MANAGEMENT RESPONSE

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