PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

Information Technology Audit: Registrar of Voters Selected Cybersecurity Controls

For the Period of December 15, 2021 Through March 8, 2022

Audit No. 2042
Report Date: September 12, 2022

Number of Recommendations

1	Critical Control Weaknesses
4	Significant Control Weakness
4	Control Findings

PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

Information Technology Audit:
Registrar of Voters Selected Cybersecurity Controls

September 12, 2022

AUDIT HIGHLIGHTS

SCOPE OF WORK	Perform an information technology audit of Registrar of Voters (ROV) selected cybersecurity controls for the period December 15, 2021 to March 8, 2022.
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.
1 CRITICAL CONTROL WEAKNESSES	
4 SIGNIFICANT CONTROL WEAKNESSES	
4 CONTROL FINDINGS	

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

AUDIT NO. 2042

PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

Audit No. 2042

September 12, 2022

To: Bob Page
Registrar of Voters

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

Subject: Information Technology Audit: Registrar of Voters Selected Cybersecurity Controls

---

We have completed an information technology audit of selected cybersecurity controls administered by Registrar of Voters for the period December 15, 2021 to March 8, 2022. 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.

Registrar of Voters 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 Registrar of Voters 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
ROV 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	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
	Gianne Morgan, CIA, CISA	Audit Manager
	Mari Elias, DPA	Administrative Services Manager

APPENDIX A: ADDITIONAL INFORMATION

OBJECTIVES	Our audit objectives were to evaluate Registrar of Voters design, implementation, and operating effectiveness of internal control to determine if IT control activities for: 1. Vulnerability management and malware defenses provide reasonable assurance the opportunity for attack is reduced. 2. Account management and access control management provide reasonable assurance of proper user and privileged account administration. 3. Data recovery and incident response provide reasonable assurance of IT service continuity.
SCOPE & METHODOLOGY	Our audit scope was limited to select high-risk cybersecurity controls at Registrar of Voters for the period December 15, 2021 to March 8, 2022. Our agile methodology included inquiry, observation, examination of documentation, and sampling of relevant items performed in a series of sprints. We collaborated with ROV management to identify key business objectives, potential risks interfering with achievement of those objectives, and key controls to mitigate those risks. A risk-prioritized audit backlog was created and available audit resources deployed for fieldwork.
EXCLUSIONS	We did not examine: (1) non-configurable components of in-scope critical applications, (2) vote center and headquarters operations, including proprietary vendor equipment, wireless communications, counting systems, data transport, and results reporting, (3) activities performed by external or third parties (e.g., OCIT, SAIC, State of California), nor (4) application controls.
PRIOR AUDIT COVERAGE	We have not issued any audit reports for ROV with a similar scope within the last ten years.
BACKGROUND	The mission of Registrar of Voters (ROV) is to provide election services for the citizens of Orange County, ensure equal access to the election process, protect the integrity of votes, and maintain a transparent, accurate, and fair process. ROV is comprised of six divisions: (1) Administrative Services, (2) Election Services, (3) Information & Technology (IT), (4) Candidate & Voter Services, (5) Community Outreach, and (6) Printing & Graphics. ROV IT's purpose is to meet the technical needs of the agency, provide cybersecurity support, and support its core business functions. ROV IT also provides data entry and files (which handle voter registration and petition processing) and is responsible for the precinct and Vote Center mapping functions.

PURPOSE & AUTHORITY	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).
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." Control systems shall 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 enhances and 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: REGISTRAR OF VOTERS MANAGEMENT RESPONSE

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