PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

Information Technology Audit: Auditor-Controller Information Technology General Controls

For the Year Ended February 28, 2018

Audit No. 1741
Report Date: March 6, 2019

Number of Recommendations

4	Critical Control Weaknesses
4	Significant Control Weaknesses
4	Control Findings

OC Board of Supervisors

Chairwoman Lisa Bartlett 5th District	Vice Chair Michelle Steel 2nd District	Supervisor Andrew Do 1st District	Vacant 3rd District	Supervisor Doug Chaffee 4th District

PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

Information Technology Audit:
Auditor-Controller Information Technology General Controls

March 6, 2019

AUDIT HIGHLIGHTS

SCOPE OF WORK	Perform an Information Technology Audit of the Auditor-Controller's information technology general controls for the year ended February 28, 2018.
RESULTS	• We found that controls over physical and logical access to data, network, programs, and applications should be improved to ensure access is appropriate, approved, managed, maintained, and adequately supported. • With exception to the CAPS+ environment, we found that controls over change management processes should be improved to ensure changes are appropriate, approved, and adequately supported. • We found that controls over computer operations were generally appropriate, adequate, and effectively managed to ensure timely and proper continuation of system processing.
RISKS	As a result of our findings, potential risks include: • Unauthorized access to and exposure of critical data and sensitive information. • Lack of accountability for database changes. • Unauthorized changes to critical applications and certain network configurations. • Loss of critical data and sensitive information.
NUMBER OF RECOMMENDATIONS 4 CRITICAL CONTROL WEAKNESSES 4 SIGNIFICANT CONTROL WEAKNESSES 4 CONTROL FINDINGS	Opportunities for enhancing internal control include: • Monitoring rogue wireless access points, developing encryption key management, and securing web application connections. • Developing a formal management user access rights certification review process. • Creating policies and procedures governing change management. • Documenting the provisioning of privileged new user access.

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

AUDIT NO. 1741

PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

Audit No. 1741

March 6, 2019

To: Eric Woolery, CPA
Auditor-Controller

From: Scott Suzuki, CPA, Assistant Director
Internal Audit Department

Subject: Information Technology Audit:
Auditor-Controller Information Technology General Controls

We have completed an Information Technology Audit of the Auditor-Controller's (A-C) information technology general controls for the year ended February 28, 2018. Due to the sensitive nature of specific findings (restricted information), only the results for Finding Nos. 3, 11, and 12 immediately follow 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.

A-C concurred with all of our recommendations and the Internal Audit Department considers management's response appropriate to the recommendations in this report.

Results of this audit will be included in a future status report submitted quarterly to the Audit Oversight Committee (AOC) and the Board of Supervisors (Board). Additionally, 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 assistance extended to us by Auditor-Controller personnel during our audit. If you have any questions, please contact me at 714.834.5509 or IT Audit Manager II Jimmy Nguyen at 714.834.2526.

Attachments

Other recipients of this report:
Members, Board of Supervisors
Members, Audit Oversight Committee
Auditor-Controller Distribution
Foreperson, Grand Jury
Robin Stieler, Clerk of the Board of Supervisors
Vavrinek, Trine, Day & CO., LLP, County External Auditor

RESULTS	
BUSINESS PROCESS & INTERNAL CONTROL STRENGTHS	Business process and internal control strengths noted during our audit include: ✓ Strong IT general controls in place over the CAPS+ environment. ✓ Strong physical security controls over the A-C server room. ✓ Auditor-Controller Information Technology Division (A-C IT) is in the process of implementing a new project management system. ✓ Timely responses and resolution of A-C IT Helpdesk tickets.

FINDING NO. 1	Removed due to the sensitive nature of the finding.

FINDING NO. 2	Removed due to the sensitive nature of the finding.

FINDING NO. 3	**Change Management Process** We reviewed changes made to the A-C network and critical applications managed by A-C IT and found an inconsistent change management process. Without a consistent change management process, we were unable to validate that critical change management steps were performed to ensure changes were appropriately reviewed, tested, and authorized prior to implementation into production. In the case of one of the applications reviewed (Virtual Timecard Interface or VTI), we found changes were also implemented into production by the third-party vendor without A-C IT management authorization.
CATEGORY	**Critical Control Weakness**
RISK	Lack of a robust change management process could result in unauthorized changes made to critical applications and certain network configurations.

RECOMMENDATION	We recommend Auditor-Controller create and implement formal change management processes including: 1) Documenting proper management review, approval, and testing of changes prior to deploying changes into the production environment. 2) Limiting vendor access to the department's production environment, where feasible. 3) Considering creation of a departmental change advisory/review board with periodic meetings to ensure that all changes are discussed, reviewed, approved, and documented prior to deployment into production. For emergency changes, the board should ensure changes are reviewed post-implementation.
MANAGEMENT RESPONSE	**Concur.** We will implement a change management process for A/C-supported applications under consideration, such as VTI, that is aligned with our team's customer-driven objectives. This includes a streamlined workflow process that documents management reviews and approvals, and a migration process, emergency or not, that transition a change from non-production to production environment. We will leverage our existing internal control process for CAPS+ and inform the Internal Control group about the changes. For vendor access to production environment, we will work with those vendors to limit and monitor their use of such privileges.

FINDING NO. 4	Removed due to the sensitive nature of the finding.

FINDING NO. 5	Removed due to the sensitive nature of the finding.

FINDING NO. 6	Removed due to the sensitive nature of the finding.

FINDING NO. 7	Removed due to the sensitive nature of the finding.

FINDING NO. 8	Removed due to the sensitive nature of the finding.

FINDING NO. 9	Removed due to the sensitive nature of the finding.

FINDING NO. 10	Removed due to the sensitive nature of the finding.

FINDING NO. 11	**Data Backup Tape Inventory Utility Access** A-C IT monitors and tracks media backup tape inventory activities through an online vendor utility. Based on a review of all user access rights to the utility, we found three of the 10 (30%) users no longer required access and were not appropriately removed. We also found that their access rights allowed them to release and receive media backup tapes from the vendor.
CATEGORY	**Control Finding**
RISK	Unnecessary access to critical data poses a heightened risk to IT security.
RECOMMENDATION	We recommend Auditor-Controller timely remove access for employees who are no longer with A-C IT or whose primary job duties no longer involve backups. Further, we recommend Auditor-Controller periodically review access to the backup tape inventory utility to ensure that access is appropriately assigned to individuals with a direct business need.
MANAGEMENT RESPONSE	**Concur.** We agree and will promptly disable user access to the online vendor utility when such user is no longer assigned data backup duties or employed at A/C. We will regularly monitor and review all user access rights to the utility to identify anomalies so corrective actions can be taken.

FINDING NO. 12	**Privileged New User Access Documentation** We found an employee that rotated into A-C IT from another County department was granted privileged access rights to the network and critical applications without properly documented management authorization.
CATEGORY	**Control Finding**
RISK	Given the heightened risks associated with cybersecurity, undocumented approvals granting privileged access to the County network significantly increases the risk of unauthorized access to County sensitive data.
RECOMMENDATION	We recommend Auditor-Controller properly document management authorization and requests for privileged new user access to network resources.

MANAGEMENT RESPONSE	**Concur.** We agree and will document management authorization and requests for privilege new user access to network resource as part of user provisioning process.

AUDIT TEAM	Jimmy Nguyen, CISA, CFE, CEH	IT Audit Manager II
	Scott Kim, CPA, CISA	IT Audit Manager I

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: 1. Ensure physical and logical access to data, network, programs, and applications was appropriate, approved, managed, maintained, and adequately supported. 2. Ensure change management processes were appropriate, approved, and adequately supported. 3. Ensure computer operations were appropriately, adequately, and effectively managed to ensure timely and proper continuation of system processing.
SCOPE & METHODOLOGY	Our audit scope was limited to selected information technology general controls over security management, change management processes, and computer operations at the Auditor-Controller for the year ended February 28, 2018. Our scope was further limited to Auditor-Controller network and critical applications managed by A-C IT. 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 OCIT nor any services/activities performed or provided by the County's managed services vendors.
PRIOR AUDIT COVERAGE	We have not issued any audit reports for A-C with a similar scope within the last ten years.
BACKGROUND	A-C'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." Annually the A-C prepares the County's Comprehensive Annual Financial Report (CAFR) which details how the County spent its budget of over $6 billion during the fiscal year. A-C IT is responsible for managing the Auditor-Controller and Countywide financial systems, which includes the Countywide Accounting and Personnel System (CAPS+). This critical system supports budget preparation and control, financial records and reporting, procurement, vendor payments and trust disbursing, cost recovery for State and Federal programs, and payroll and personnel records. Other critical systems managed include the document imaging and management system (ERMI), Virtual Timecard Interface (VTI), Mileage Claim & Parking, and Paystub Portal.

INTERNAL AUDIT DEPARTMENT

PURPOSE & AUTHORITY	We performed this audit in accordance with the FY 2018-19 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 and Control Objectives for Information and Related Technologies issued by the Information Systems Audit and Control Association.
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 CLASSIFICATIONS

Critical Control Weaknesses	Significant Control Weaknesses	Control Findings
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: AUDITOR-CONTROLLER MANAGEMENT RESPONSE

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