PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

Information Technology Audit:
Social Services Agency
IT Logical Security & Change Management

For the Year Ended March 31, 2019

Audit No. 1846
Report Date: October 23, 2019

Number of Recommendations

1	Critical Control Weaknesses
4	Significant Control Weaknesses
4	Control Findings

OC Board of Supervisors

Chairwoman Lisa A. Bartlett	Vice Chair Michelle Steel	Supervisor Andrew Do	Supervisor Donald P. Wagner	Supervisor Doug Chaffee
5th District	2nd District	1st District	3rd District	4th District

PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

Information Technology Audit:
Social Services Agency IT Logical Security & Change Management

October 23, 2019

AUDIT HIGHLIGHTS

SCOPE OF WORK	Perform an Information Technology Audit of the Social Services Agency (SSA) IT logical security & change management controls as of March 31, 2019.
RESULTS	• We concluded that SSA's internal control over logical access to department critical systems should be improved to ensure access is appropriate, privileged access is granted only to authorized individuals, and access is revoked timely upon termination. • We concluded that SSA's internal control over changes to critical systems should be improved to ensure changes are authorized and appropriately tested before deployment into production.
RISKS	As a result of our findings, potential risks include: • Unauthorized access to and/or exposure of sensitive data. • Lack of accountability for department staff use of certain critical systems. • Unauthorized and untested changes to certain department critical systems. • Lack of understanding of critical IT processes, potential cybersecurity violations, and delayed system implementations.
NUMBER OF RECOMMENDATIONS 1 CRITICAL CONTROL WEAKNESSES 4 SIGNIFICANT CONTROL WEAKNESSES 4 CONTROL FINDINGS	Opportunities for enhancing internal control include: • Creating policy and procedures governing access management to sensitive IT areas, privileged user access certification review, and change management. • Eliminating or reducing the number of generic accounts. • Changing vendor default user account configurations to database systems.

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

AUDIT NO. 1846

PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

Audit No. 1846

October 23, 2019

To: Debra J. Baetz, Director
Social Services Agency

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

Subject: Information Technology Audit: Social Services Agency IT Logical Security & Change Management

---

We have completed an Information Technology Audit of the Social Services Agency IT logical security and change management controls as of March 31, 2019. Due to the sensitive nature of specific findings (restricted information), only the results for Finding Nos. 7, 8, and 9 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.

SSA concurred with all of 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 Social Services Agency 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
SSA 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: ✓ Strong controls over user access management for certain department critical systems reviewed. ✓ Strong review controls for case-management activities for a critical system. ✓ Dual authorization is required and documented prior to granting access for specific department critical systems.

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	Removed due to the sensitive nature of the finding.

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	**Change Testing Documentation** For one of the five (20%) changes selected and tested, there was a lack of documentation or information to evidence that testing of changes were performed prior to deployment into the production environment. SSA indicated that testing was performed for this change but did not document the test plan and results.
CATEGORY	**Control Finding**
RISK	Lack of documentation or information to evidence testing occurred increases the risk that changes were not appropriately tested prior to deployment into the production environment. Testing changes in a test environment helps to minimize disruptions or any adverse effects to critical business operations.
RECOMMENDATION	SSA ensure appropriate testing documentation is created, reviewed, and maintained for all changes prior to deployment into the production environment.
MANAGEMENT RESPONSE	**Concur.** SSA will ensure appropriate testing documentation for changes prior to deployment into production. To facilitate the documentation, review and authorization process prior to production, SSA has created a change management procedure. This procedure specifically addresses test plan development, approval and documentation.

FINDING NO. 8	**Department IT Policy & Procedures** We noted SSA lacked up-to-date documented IT policy and procedures governing IT business processes over critical systems that included: • Provisioning of new user access requests to critical systems. • Managing and monitoring privileged (administrative) user accounts for appropriateness. • De-provisioning of user access to critical systems upon employee termination. • Change management, e.g., change requests to critical systems must be documented, adequately tested, and approved prior to deploying changes into production. SSA has department-wide policy and procedures over user access to the network. In addition, although there are no uniform procedures in place over user access management to critical applications. The lack of uniform procedures causes inefficiencies in the implementation of controls across the department. For example: • Some applications tested required that forms be completed for access changes (i.e., provision and de-provision) while others did not. • Some applications had different document retention requirements. • Some applications required multiple levels of management review and authorization, while others of similar risk did not. Different forms, review steps, and documentation retention policies resulted in varying levels of completeness, accuracy, and strength of tested controls across the critical applications tested.
CATEGORY	**Control Finding**
RISK	Lack of IT policy and procedures can result in a lack of understanding of IT business processes, cybersecurity violations, and delayed implementation of systems.
RECOMMENDATION	SSA develop comprehensive IT policy and procedures that govern the areas of provisioning/de-provisioning user access, managing privileged user access rights, and change-management to critical systems.
MANAGEMENT RESPONSE	**Concur.** SSA will update its IT policy and procedures that govern the areas of provisioning/de-provisioning user access, managing privileged user access rights, and change management to critical systems.

FINDING NO. 9	**Access Provisioning Documentation and Authorization** One of 13 users (8%) we sampled for new user access provisioning did not have documentation to evidence that access was authorized prior to provisioning access.
CATEGORY	**Control Finding**
RISK	Unauthorized access to critical systems could result due to a lack of consistent documentation of review and authorization prior to provisioning access.
RECOMMENDATION	SSA ensure new user access to critical applications is documented, and include evidence of appropriate authorization and review prior to provisioning user access rights.
MANAGEMENT RESPONSE	**Concur.** SSA will ensure new user access to critical applications is documented and include evidence of appropriate authorization and review prior to provisioning user access rights. To facilitate this effort, the department is in the process of consolidating unique divisional user access request forms into a single form including authorization which will provide agency wide consistency of user provisioning.

AUDIT TEAM	Scott Suzuki, CPA, CIA, CISA	Assistant Director
	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 assess internal control over: 1. Logical access to department critical systems to ensure access is appropriate, privileged access is granted only to authorized individuals, and access is revoked timely upon termination. 2. Changes to critical systems to ensure changes are authorized and appropriately tested before deployment into production.
SCOPE & METHODOLOGY	Our audit scope was limited to selected high risk information technology general controls over logical security management and change management at the Social Services Agency (SSA) as of March 31, 2019. Our methodology included inquiry, observation, examination of documentation, and sampling of relevant items.
EXCLUSIONS	We did not examine application controls or any processes administered by external parties such as OCIT nor any services/activities performed or provided by the County's or State of California's third-party vendors.
PRIOR AUDIT COVERAGE	We have not issued any audit reports for SSA with a similar scope within the last ten years.
BACKGROUND	SSA's mission is to deliver quality services that are accessible and responsive to the community, encourage personal responsibility, strengthen individuals, preserve families, and protect vulnerable adults and children. SSA administers Federal, State, and County social services programs that protect children and adults from abuse or neglect, enable the frail and disabled to remain in their homes rather than being institutionalized; move eligible families from dependency to self-sufficiency; and provide benefits for eligible CalWORKs, CalFresh, Refugee, General Relief, and Medi-Cal recipients. SSA manages and supports various systems that handle sensitive information such as child welfare cases, eligibility benefits, and tracking welfare payments.

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.
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: SOCIAL SERVICES AGENCY MANAGEMENT RESPONSE

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