PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

Information Technology Audit: Sheriff-Coroner Selected IT General Controls

For the Year Ended June 30, 2019

Audit No. 1845
Report Date: December 30, 2019

Number of Recommendations

0	Critical Control Weaknesses
6	Significant Control Weaknesses
1	Control Findings

PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

Information Technology Audit:
Sheriff-Coroner Selected IT General Controls

December 30, 2019

AUDIT HIGHLIGHTS

SCOPE OF WORK	Perform an Information Technology Audit of Sheriff-Coroner selected IT general controls for the year ended June 30, 2019.
RESULTS	• We concluded controls over access to critical systems should be improved. • We concluded controls were generally effective to provide reasonable assurance that physical access to IT server rooms or other sensitive IT areas is limited to authorized individuals. • We concluded controls over changes to critical systems should be improved.
RISKS	As a result of our findings, potential risks include: • Unauthorized access to, and exposure of, sensitive data. • Lack of accountability for department staff use of certain critical systems. • Unauthorized or untested changes to critical systems.
NUMBER OF RECOMMENDATIONS 0 CRITICAL CONTROL WEAKNESSES 6 SIGNIFICANT CONTROL WEAKNESSES 1 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. • Creating a uniform new user access request process for all critical systems. • Changing/disabling default vendor account IDs. • Eliminating or reducing the number of generic accounts. • Ensuring changes are appropriately documented, reviewed, and authorized. • Performing periodic user access certification reviews. • Conducting periodic change advisory meetings.

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

AUDIT NO. 1845

PUBLIC INFORMATION

INTERNAL AUDIT DEPARTMENT

Audit No. 1845

December 30, 2019

To: Don Barnes
Sheriff-Coroner

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

Subject: Information Technology Audit: Sheriff-Coroner Selected IT General Controls

---

We have completed an Information Technology Audit of the Sheriff-Coroner (OCSD) selected IT general controls for the year ended June 30, 2019. Due to the sensitive nature of specific findings (restricted information), only the results for Finding Nos. 6 and 7 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.

OCSD 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 Sheriff-Coroner 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
OCSD 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 to the OCSD network. ✓ Automatic disabling of user access rights upon periods of user inactivity for some OCSD applications. ✓ Physical security assessment performed by third-party vendor that resulted in minimal findings. ✓ Visitors are required to check in. ✓ Implemented security software utility that monitors network privileged account utilization for suspicious activities.
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	**Testing of Changes Before Deployment Into Production** OCSD indicated changes were tested prior to deployment into production. However, none of the six (0%) changes to the tested critical application production environment or network had support documentation to evidence that testing of changes was done prior to deployment into the production environment.

CATEGORY	**Significant Control Weakness**
RISK	Lack of documentation or information to evidence testing in a test environment increases the risk that changes were not appropriately tested prior to deployment into the production environment in order to minimize disruptions or any adverse effects to critical business operations.
RECOMMENDATION	OCSD ensure that test plan documentation is created and maintained to evidence that changes are being tested and reviewed prior to deployment into the production environment.
MANAGEMENT RESPONSE	**[Concur.]** All changes are reviewed, tested, and approved by management and affected departments before execution. OCSD IT has an active project to modernize our ITSM and change management application which will bring improvements and formality in the way we track and document change requests to the sheriff network and applications.

FINDING NO. 7	**Department IT Policies & Procedures** We noted OCSD lacks documented IT policy and procedures governing various IT business processes over critical systems that include: • Provisioning of new user access requests to critical systems. • Managing and monitoring privileged (administrative rights) user accounts for appropriateness. • Deprovisioning of user access to critical systems upon employee termination. • Change Management – Change requests to critical systems must be documented, adequately tested, and approved, prior to deploying changes into production.
CATEGORY	**Control Finding**
RISK	Lack of IT policies and procedures can result in a lack of understanding of IT business processes, cyber security violations, and delayed implementation of systems.
RECOMMENDATION	OCSD 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.]** OCSD IT is actively working on updating existing documentation and introducing new documentation to address any gaps. We also work closely with County IT and participate in the County Cyber Security Joint Task Force and Tech Council tasked with developing documentation that will apply to all county agencies.

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 determine if selected OCSD IT general controls: 1. Provide reasonable assurance that access to critical systems is limited to authorized individuals. 2. Provide reasonable assurance that physical access to IT server rooms or other sensitive IT areas is limited to authorized individuals. 3. Provide reasonable assurance that changes to critical systems are authorized and appropriately tested before being deployed into production.
SCOPE & METHODOLOGY	Our audit scope was limited to selected high risk information technology general controls over security and change management at OCSD for the year ended June 30, 2019. 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	We issued Information Technology Audit: Sheriff-Coroner Computer General Controls, Audit No. 1353, on January 13, 2015.
BACKGROUND	OCSD is a large, multi-faceted law enforcement agency served by approximately 3,800 sworn and professional staff members and over 800 reserve personnel. The department consists of five organizational Commands comprised of 21 separate Divisions: • **Executive Command** – includes Sheriff's Executive Management, Community Services and Media/Government Relations. • **Administrative Services Command** – includes Communications, Financial/Administrative Services, Research & Development and Support Services. • **Custody Operations & Court Services Command** – includes the three Jail Facilities, Inmate Services and Court Operations. • **Field Operations & Investigative Services Command** – includes Airport Operations, Homeland Security, North and South Patrol Operations and Investigations, Coroner, Emergency Communications, Crime Lab, and Reserve & Volunteer Bureau • **Professional Services Command** – includes Court Operations, Professional Standards, S.A.F.E., Training, and Community Programs. Sheriff-Coroner operates an in-house IT division department that manages and/or supports various critical systems. The Sheriff-Coroner IT division is separate from the County centralized IT functions and is not part of the Managed and Shared Services model.

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: OC SHERIFF'S DEPARTMENT MANAGEMENT RESPONSE

ORANGE COUNTY
SHERIFF'S DEPARTMENT

EXTERNAL MEMO

To: Director Aggie Alonso, Internal Audit Department
From: Director Kirk Wilkerson, Support Services Division
Date: December 23, 2019
RE: Information Technology Audit: Sheriff-Coroner Selected IT General Controls

Director Alonso,

We received the *Sheriff-Coroner Selected IT General Controls audit report* detailing results from the work conducted by your department in June, 2019. We have reviewed the draft report and agree with the findings identified in the document. Included below is our responses for each finding in order to add additional context and to document the actions we will take to address each item.

Finding No 1

[redacted]

Finding No 2

[redacted]

Finding No 3

[redacted]

Finding No 4

[redacted]

Finding No 5

[redacted]

Finding No 6

All changes are reviewed, tested, and approved by management and affected departments before execution. OCSD IT has an active project to modernize our ITSM and change management application which will bring improvements and formality in the way we track and document change requests to the sheriff network and applications.

Integrity without compromise | Service above self | Professionalism in the performance of duty | Vigilance in safeguarding our community

ORANGE COUNTY SHERIFF'S DEPARTMENT
EXTERNAL MEMO

Finding No 7

OCSD IT is actively working on updating existing documentation and introducing new documentation to address any gaps. We also work closely with County IT and participate in the County Cyber Security Joint Task Force and Tech Council tasked with developing documentation that will apply to all county agencies.

Thank you for this report. Protecting the Sheriff's network is our top priority, which requires that we continuously review and revise our practices to adapt to an ever-changing security landscape - it is always helpful to have a second set of eyes review our processes to ensure we are being as diligent as possible in the protection of our network and data. We appreciate your staff's commitment and professionalism during this engagement and look forward to working with them again in the future.