ORANGE COUNTY

AUDITOR-CONTROLLER

INTERNAL AUDIT

SECOND FOLLOW-UP INFORMATION TECHNOLOGY AUDIT:

SHERIFF-CORONER COMPUTER GENERAL CONTROLS

As of August 15, 2016

ORANGE COUNTY AUDITOR-CONTROLLER ★ CALIFORNIA ★

Audit Number #1353-F2
Reference (1652)
Report Date: August 30, 2016

ORANGE COUNTY

AUDITOR-CONTROLLER

INTERNAL AUDIT

Eric H. Woolery, CPA
Orange County Auditor-Controller

Toni Smart, CPA	Director, Internal Audit
Scott Suzuki, CPA, CIA, CISA	Assistant Director
Jimmy Nguyen, CISA, CFE	IT Audit Manager I
Scott Kim, CPA	Senior Auditor

12 Civic Center Plaza, Room 200
Santa Ana, CA 92701

Auditor-Controller Web Site
www.ac.ocgov.com

ERIC H. WOOLERY, CPA
AUDITOR-CONTROLLER

Transmittal Letter

Audit No. 1353-F2
(Reference 1652)

August 30, 2016

TO: Sandra Hutchens
Sheriff-Coroner

SUBJECT: Second Follow-Up Information Technology Audit:
Sheriff-Coroner Computer General Controls, Original Audit 1353, Issued January 13, 2015

We have completed our Second Follow-Up Information Technology Audit of Sheriff-Coroner Computer General Controls as of August 15, 2016. Our final report is attached for your review.

I submit an **Audit Status Report** quarterly to the Audit Oversight Committee (AOC) and a monthly report to the Board of Supervisors (BOS) where I detail any critical and significant audit findings released in reports during the prior month and the implementation status of audit recommendations as disclosed by our Follow-Up Audits. Accordingly, the results of this assessment will be included in a future status report to the AOC and BOS.

Toni Smart

Toni Smart, CPA, Director
Auditor-Controller Internal Audit Division

Attachment

Other recipients of this report:
Members, Board of Supervisors
Members, Audit Oversight Committee
Eric Woolery, Auditor-Controller
Frank Kim, County Executive Officer
Don Barnes, Undersheriff, OCSD
Brian Wayt, Executive Director, Administrative Services Command, OCSD
Robert Beaver, Senior Director, Administrative Services Command, OCSD
Noma Crook, Director, Financial/Administrative Services Division, OCSD
Kirk Wilkerson, Director, Support Services Division, OCSD
Foreperson, Grand Jury
Robin Stieler, Clerk of the Board of Supervisors
Macias Gini & O’Connell LLP, County External Auditor

Table of Contents

Second Follow-Up Information Technology Audit:
Sheriff-Coroner Computer General Controls
Audit No. 1353-F2 (Reference 1652)

As of August 15, 2016

Internal Auditor's Report

Audit No. 1353-F2 **August 30, 2016**

TO: Sandra Hutchens
Sheriff-Coroner

FROM: Toni Smart, CPA, Director
Auditor-Controller Internal Audit Division

SUBJECT: Second Follow-Up Information Technology Audit:
Sheriff-Coroner Computer General Controls, Original Audit 1353, Issued January 13, 2015

SCOPE

We have completed a Second Follow-Up Information Technology Audit of Sheriff-Coroner (OCSD) Computer General Controls. Our audit was limited to reviewing actions taken as of August 15, 2016, to implement the remaining **three (3) recommendations** from our First Follow-Up Audit report dated October 22, 2015.

BACKGROUND

The original audit found IT general controls were adequate and identified **four (4) Control Findings** to enhance the Sheriff-Coroner's computer general controls. General controls are the structure, policies, and procedures that apply to an entity's overall computer operations. If general controls are weak, they severely diminish the reliability of controls associated with individual applications. Sheriff-Coroner/Information Systems Bureau utilizes a number of systems that store and process sensitive/confidential data including law enforcement operations involving criminal investigations, jail operations, undercover and forensic work. In addition, these systems interface with other key statewide and Department of Justice law enforcement systems. Therefore, restricting access to the systems and data is a key priority.

RESULTS

Our Second Follow-Up Audit indicated that the Sheriff-Coroner **implemented two (2) recommendations and is in process of implementing one (1) recommendation.** Because this is our second follow-up audit, the recommendation not fully implemented will be reported to the Audit Oversight Committee in a quarterly status report.

Based on our First and Second Follow-Up Audits, the following is the implementation status of three (3) of the original recommendations:

1. Finding No. 1 – Security Settings May Be Improved (Control Finding)

Recommendation No. 1: Sheriff-Coroner should consider changing the security settings to meet best practices.

Current Status: **Implemented.** Our First Follow-Up Audit found the Sheriff-Coroner revised the network security settings to better align with access security best practices. Because network security settings were revised to meet best practices, we consider this recommendation implemented.

2. Finding No. 2 – Change Control Policies and Procedures Need to be Developed (Control Finding)

Recommendation No. 2: Sheriff-Coroner should develop policies and procedures to address: vendor supplied passwords, embedded passwords, development environment, changes to network devices, personal and public domain software, and patch management.

Current Status: **Implemented.** Our Second Follow-Up Audit found that OCSD IT policies and procedures governing vendor supplied passwords, embedded passwords, development environment, changes to network devices, personal and public domain software, and patch management are appropriately established, documented and updated to meet current best practices and is reviewed by management upon any revisions as needed. Because the OCSD IT Computer Operations policies and procedures document is appropriately maintained and updated to reflect current IT processes as well as best practices, we consider this recommendation implemented.

3. Finding No. 3 – Computer Operations Policies and Procedures Need to be Developed (Control Finding)

Recommendation No. 3: Sheriff-Coroner should document and maintain its computer operation policies and procedures.

Current Status: **Implemented.** Our Second Follow-Up Audit found that the OCSD IT Operations Manual document is appropriately updated to meet current best practices and is reviewed by management upon any revisions. Additionally, the document is designed as a supplement that leverages off of the Countywide IT Usage Policy as well as the CJIS (Criminal Justice Information Systems) Security policy. Because the OCSD IT Computer Operations policies and procedures document is appropriately maintained, established and documented to reflect current IT processes as well as best practices, we consider this recommendation implemented.

4. Finding No. 4 – Contingency Plans Need to Be Updated and Tested (Control Finding)

Recommendation No. 4: Sheriff-Coroner should develop a plan for testing its disaster recovery and contingency plans on a regular basis.

Current Status: **In process.** Our Second Follow-Up Audit found that the implementation of the IT Disaster Recovery (DR) and Business Continuity Plan (BCP) are currently in progress, with the first of three (3) phases scheduled to be completed by January 2017, addressing critical mainframe applications and email. Phase II is scheduled to be completed by August 2017 which will complete the Open System Disaster Recovery. Phase III is scheduled to be completed by December 2017 which will finish the Secondary Wide Area Network (WAN) Connectivity Hot Site. Although the contingency plan is in process, OCSD has incorporated the following key activities:

1) Employed a full-time project manager dedicated to the IT DR/BCP plan project deployment.

2) Developed a management approved, detailed IT DR Planning document that outlines critical areas such as executive summary, defining critical in-scope applications, deliverables & various phases.
3) Contracted with the California Department of Justice (DOJ) Data Center to serve as the off-site OCSD Disaster Recovery location.
4) Network hardware equipment procurement is in progress.
5) The backup mainframe system is scheduled to be shipped and installed at the CA DOJ Data Center facility.
6) The WAN connectivity to the CA DOJ Data Center facility is scheduled to be installed and activated.

Because the IT DRP and BCP is in the process of being developed, we consider this recommendation in process.

We appreciate the assistance extended to us by Sheriff-Coroner personnel during our Follow-Up Audit. If you have any questions, please contact me directly at 714-834-5442 or Scott Suzuki, Assistant Director at 714-834-5509.