Orange County Auditor-Controller

Internal Audit

General Assessment of Auditor-Controller Information Technology Security As of June 30, 2016

Audit Number 1543
Report Date: November 15, 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**

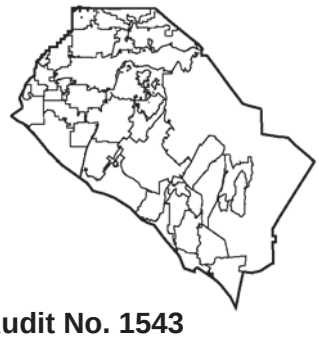
12 Civic Center Plaza, Room 200

Santa Ana, CA 92701

Auditor-Controller Web Site

www.ac.ocgov.com

ERIC H. WOOLERY, CPA
AUDITOR-CONTROLLER



Transmittal Letter

Audit No. 1543

November 15, 2016

TO: Eric H. Woolery, CPA
Auditor-Controller

SUBJECT: General Assessment of Auditor-Controller IT Security

We have completed an informal general assessment of IT security at the Auditor-Controller's Office as of June 30, 2016. **Due to the sensitive nature of the specific findings, a modified version of the 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, CPA, Director
Auditor-Controller Internal Audit Division

Attachments

Other recipients of this report:
Members, Board of Supervisors
Members, Audit Oversight Committee
Frank Kim, County Executive Officer
Phil Daigneau, Director of Information Technology, Auditor-Controller
Foreperson, Grand Jury
Robin Stieler, Clerk of the Board of Supervisors
Macias Gini & O'Connell LLP, County External Auditor

Table of Contents

General Assessment of Auditor-Controller
Information Technology Security
Audit No. 1543

As of June 30, 2016

Internal Auditor's Report

Audit No. 1543 **November 15, 2016**

TO: Eric H. Woolery, CPA
Auditor-Controller

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

SUBJECT: General Assessment of Auditor-Controller Information Technology Security

OBJECTIVES

The purpose of this general assessment was to bring to Auditor-Controller management's attention important issues related to information technology security for evaluation and corrective action. This general assessment is of advisory nature and is not subject to the same rigor and formality of a traditional report in that we have not fully developed the issues. Therefore, this assessment does not constitute a complete audit of the Auditor-Controller Information Technology (A-C/IT) Division.

RESULTS

Our assessment revealed eight (8) IT security findings, including **one (1) Critical Control Weakness** and **four (4) Significant Control Weaknesses** that involve Network Security Configurations. The remaining **three (3) Control Findings** deal with Information Technology Security Policies. The results of this assessment will be considered in the A-C Internal Audit Division's risk analysis when preparing future audit plans. **Due to the sensitive nature of the specific findings, the details of the report were presented to a limited audience**.

BACKGROUND

A-C/IT is one of five divisions within the Office of the Auditor-Controller. The division is charged with managing IT services for Auditor-Controller and Treasurer-Tax Collector (T-TC) employees, training rooms, conference rooms, as well as administering logical access to servers, databases, and applications, developing and maintaining applications, and maintaining related hardware (desktop, printers, scanners, cell phones). T-TC IT services are provided by the A-C under agreement with the Office of the T-TC.

SCOPE AND METHODOLOGY

The scope of our informal assessment was limited to a desk audit of IT security within the Auditor-Controller's local area network as of June 30, 2016. To accomplish the assessment's objectives, we utilized standard IT audit tools to query the network and conducted discussions with A-C/IT staff.

Scope Exclusions. Our assessment was generally limited to one division in the Auditor-Controller operations and did not include review of applications, database security, system development/change management, or disaster recovery/business continuity.

MANAGEMENT'S RESPONSIBILITIES FOR INTERNAL CONTROLS

In accordance with the Auditor-Controller's County Accounting Manual Section 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 an entity's internal control structure is the Committee of Sponsoring Organizations (COSO) control framework. Our Internal Control Audit enhances and complements, but does not substitute for the A-C's continuing emphasis on control activities and self-assessment of control risks.

Inherent Limitations in Any System of Internal Control

Because of inherent limitations in any system of internal controls, 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 A-C's operating procedures, accounting practices, and compliance with County policy.

ACKNOWLEDGEMENT

We appreciate the courtesy extended to us by the personnel of the Auditor-Controller Information Technology Division during our audit. If you have any questions regarding our audit, please contact me directly at (714) 834-5442, or Scott Suzuki, Assistant Director at (714) 834-5509.

ATTACHMENT A: Report Item Classifications

For purposes of reporting our audit findings and recommendations, we will classify audit report items into three distinct categories:

- **Critical Control Weaknesses:**
  These are Audit Findings or a combination of Auditing 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 their attention immediately.

- **Significant Control Weaknesses:**
  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.

- **Control Findings:**
  These are Audit Findings concerning internal controls, compliance issues, or efficiency/effectiveness issues that require management's corrective action to implement or enhance processes and internal controls. Control Findings are expected to be addressed within our follow-up process of six months, but no later than twelve months.