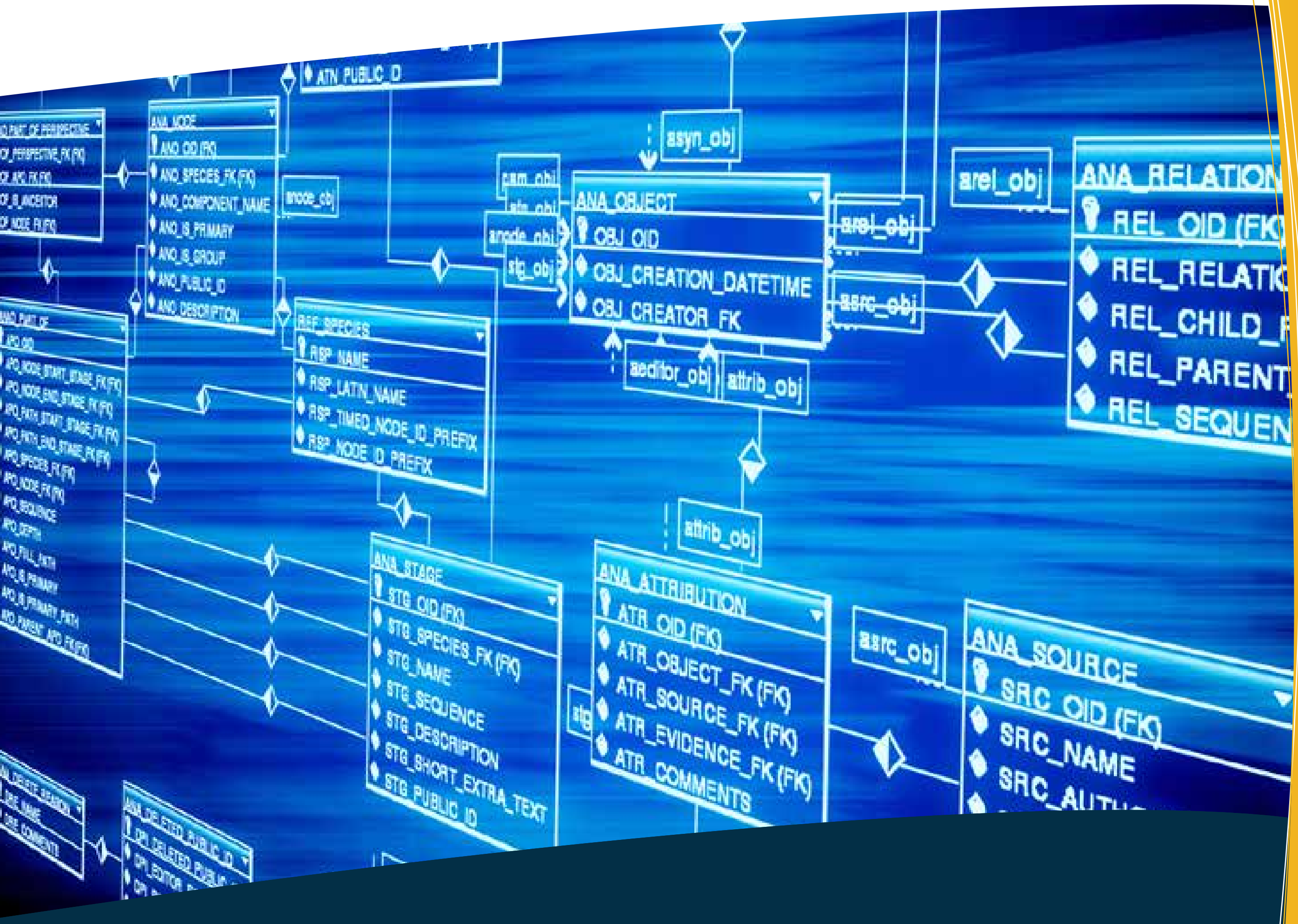
Orange County Auditor-Controller
Internal Audit



Second Follow-Up Information Technology Audit:
Access Request Application
Using Computer-Assisted Audit Techniques:
Auditor-Controller

As of November 1, 2017

Audit Number 1652 (Reference 1357-F2)

Report Date: February 27, 2018

ORANGE COUNTY

AUDITOR-CONTROLLER

INTERNAL AUDIT

Eric H. Woolery, CPA

Orange County Auditor-Controller

Scott Suzuki, CPA, CIA, CISA	**Director of Internal Audit**
Jimmy Nguyen, CISA, CFE	**IT Audit Manager II**

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. 1652
(Reference 1357-F2)

February 27, 2018

TO: Eric H. Woolery, CPA
Auditor-Controller

SUBJECT: Second and Final Close-Out Follow-Up Information Technology Audit: Access Request Application Using Computer-Assisted Audit Techniques: Auditor-Controller, Original Audit 1357, Issued August 20, 2014

We have completed our Second and Final Close-Out Follow-Up Information Technology Audit Access Request Application (ARA) using Computer-Assisted Audit Techniques (CAATs) as of November 1, 2017. Our final report is attached for your review.

An **Audit Status Report** is submitted quarterly to the Audit Oversight Committee (AOC) and the Board of Supervisors (BOS) detailing any critical and significant audit findings released in reports during the prior quarter 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.

Scott Suzuki, CPA, Director
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
Lawrence McCabe, Administrative Manager III, Auditor-Controller
Foreperson, Grand Jury
Robin Stieler, Clerk of the Board of Supervisors
Macias Gini & O’Connell LLP, County External Auditor

Table of Contents

Second and Final Close-Out Follow-Up
Information Technology Audit:
Access Request Application (ARA) Using
Computer-Assisted Audit Techniques (CAATS)
Audit No. 1652 (Reference 1357-F2)

As of November 1, 2017

Internal Auditor's Report

Audit No. 1652
(Reference 1357-F2)

February 27, 2018

TO: Eric H. Woolery, CPA
Auditor-Controller

FROM: Scott Suzuki, CPA, Director
Internal Audit Division

SUBJECT: Second and Final Close-Out Follow-Up Information Technology Audit:
Access Request Application Using Computer-Assisted Audit Techniques:
Auditor-Controller, Original Audit No. 1357, Issued August 20, 2014

SCOPE

We have completed a Second and Final Close-Out Follow-Up Information Technology Audit of Audit Access Request Application (ARA) using Computer-Assisted Audit Techniques (CAATs). Our audit was limited to reviewing actions taken as of November 1, 2017, to implement the **three (3) recommendations** from our First Follow-Up Audit No. 1357-F1, issued July 31, 2015.

BACKGROUND

We conducted the original audit to: (1) review ARA design documents to identify application controls, (2) analyze CAPS+ user access to identify policy conflicts, (3) compare CAPS+ user accounts with HR employee files to identify inappropriate access, and (4) analyze CAPS+ security tables to identify inefficiencies. The original audit identified **three (3) Control Findings**.

RESULTS

Our Second Follow-Up Audit found that the Auditor-Controller **implemented two (2) recommendations** and a third recommendation was closed. As such, this report represents the final close-out of the original audit.

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

Finding No. 1 – Security and Workflow Policy Conflicts (Control Finding)

Recommendation No. 1: The Auditor-Controller should research and validate the reported exceptions. For any policy conflicts, the identified accounts' access should be modified to eliminate the conflict.

Current Status: **Closed.** Our Second Follow-Up Audit found the Auditor-Controller implemented a department policy governing CAPS+ Security & Workflow which outlines management responsibilities for maintaining proper Segregation of Duties (SoD) in Security & Workflow. In addition, we found the SoD user access security matrix is discussed, reviewed, and approved for appropriateness on an annual basis during the Internal Controls Working Group meeting.

For the legacy SoD user access that had conflicts and were migrated into the new system, we found that although these conflicts remained, there are robust mitigating controls enforced by the system. These controls do not allow a single user the authority to initiate, submit, and approve a single transaction as evidenced by our observation walkthroughs and inspection of supporting documentation.

In addition, we noted that a memorandum outlining the legacy SoD conflicts, as well as the aforementioned mitigating controls, was reviewed and approved by the Auditor-Controller.

Because the Auditor-Controller implemented a standard policy governing the oversight of SoD, enforces various mitigating controls to monitor and resolve potential SoD user access conflicts (Security & Workflow), and has documented the acceptance of known risks, we consider this recommendation closed.

Finding No. 2 – CAPS+ User Account Exceptions to HR Employee Records (Control Finding)

Recommendation No. 2: The Auditor-Controller should research and validate the reported exceptions. For any valid exceptions, the accounts should be reviewed to ensure they are necessary.

Current Status: **Implemented.** Our Second Follow-Up Audit found that Auditor-Controller performed adequate research and review of CAPS+ user access roles for appropriateness. Based on the findings from the first follow-up audit, we performed a comprehensive sampling review for each area that included observation walkthroughs with Auditor-Controller/Information Technology (A-C/IT) personnel, as well as inspection of supporting documentation. We verified whether user access accounts identified were deemed appropriate and assigned with a direct business need, and accounts no longer requiring such access were immediately revoked.

Because the Auditor-Controller appropriately performed a review and disabled user accounts as a result of the exceptions identified, as well as configured the system to enforce a standard user naming convention in accordance with the department policy, we consider this recommendation implemented.

Finding No. 3 – CAPS+ Security Table Configuration (Control Finding)

Recommendation No. 3: The Auditor-Controller should research the reported exceptions and remove any unnecessary items.

Current Status: **Implemented.** Our Second Follow-Up Audit found that Auditor-Controller performed adequate research and review of CAPS+ security table configurations for appropriateness. Based on the findings from the first follow-up audit, we performed a comprehensive sampling review for each area that included observation walkthroughs with A-C/IT personnel, as well as inspection of support documentation.

We verified whether security and workflow roles identified were deemed appropriate, assigned to applicable business resources, and roles no longer granting access were immediately rescinded.

Because the Auditor-Controller appropriately performed a review and disabled appropriate security and workflow roles, we consider this recommendation implemented.

We appreciate the assistance extended to us by Auditor-Controller personnel during our Follow-Up Audit. If you have any questions, please contact me directly at (714) 834-5509.

ATTACHMENT A: Follow-Up Audit Implementation Status

For purposes of reporting the implementation status of our audit recommendations, we utilize four distinct categories:

Implemented	In Process	Not Implemented	Closed
The department has implemented our recommendation in all respects as verified by the follow-up audit. No further follow-up is required.	The department is in the process of implementing our recommendation. Additional follow-up may be required.	The department has taken no action to implement our recommendation. Additional follow-up may be required.	Circumstances have changed surrounding our original finding/ recommendation that: (1) make it no longer applicable or (2) the department has implemented and will only implement a portion of our recommendation. No further follow-up is required.