FIRST FOLLOW-UP AUDIT - ACCESS REQUEST APPLICATION (ARA) AUDIT USING COMPUTER-ASSISTED AUDIT TECHNIQUES (CAATS):

AUDITOR-CONTROLLER

AS OF APRIL 22, 2015

Our First Follow-Up Audit found Auditor-Controller has partially implemented three (3) recommendations from our original audit report dated August 20, 2014.

We analyzed 3,075 CAPS+ user accounts as of April 22, 2015, to identify potential segregation of duties conflicts, inappropriate user access, and CAPS+ security table issues.

AUDIT NO: 1357-F1
(REFERENCE 1447)
(ORIGINAL AUDIT NO. 1357)

REPORT DATE: JULY 31, 2015

Director: Dr. Peter Hughes, MBA, CPA, CITP
Assistant Director: Michael Goodwin, CPA, CIA
IT Audit Manager: Wilson Crider, CPA, CISA

Independence Objectivity Integrity

ORANGE COUNTY BOARD OF SUPERVISORS' Internal Audit Department

GAO & IIA Peer Review Compliant - 2001, 2004, 2007, 2010, 2013

Providing Facts and Perspectives Countywide

RISK BASED AUDITING

Dr. Peter Hughes **Ph.D., MBA, CPA, CCEP, CITP, CIA, CFE, CFF, CGMA**
Director
Certified Compliance & Ethics Professional (CCEP)
Certified Information Technology Professional (CITP)
Certified Internal Auditor (CIA)
Certified Fraud Examiner (CFE)
Certified in Financial Forensics (CFF)
Chartered Global Management Accountant (CGMA)
E-mail: peter.hughes@iad.ocgov.com

Michael Goodwin **CPA, CIA**
Assistant Director

Alan Marcum **MBA, CPA, CIA, CFE**
Senior Audit Manager

Autumn McKinney **CPA, CIA, CISA, CGFM**
Senior Audit Manager
Certified Information Systems Auditor (CISA)
Certified Financial Government Manager (CGFM)

Hall of Finance & Records

12 Civic Center Plaza, Room 232
Santa Ana, CA 92701

Phone: (714) 834-5475 Fax: (714) 834-2880

To access and view audit reports or obtain additional information about the OC Internal Audit Department, visit our website: www.ocgov.com/audit

OC Fraud Hotline (714) 834-3608

Letter from Dr. Peter Hughes, CPA

Transmittal Letter

Audit No. 1357-F1 **July 31, 2015**

TO: Eric Woolery, CPA
Auditor-Controller

FROM: Dr. Peter Hughes, CPA, Director
Internal Audit Department

SUBJECT: First Follow-Up Audit - Access Request Application (ARA) Using Computer-Assisted Audit Techniques (CAATs):
Auditor-Controller Original Audit No. 1357
Issued August 20, 2014

We have completed a First Follow-Up Audit of Access Request Application (ARA) Using Computer-Assisted Audit Techniques (CAATs). Our audit was limited to reviewing, as of April 22, 2015, actions taken to implement the **three (3) recommendations** from our original audit report dated August 20, 2014. We conducted this First Follow-Up Audit in accordance with the *FY 14-15 Audit Plan and Risk Assessment* approved by the Audit Oversight Committee and Board of Supervisors (BOS).

The results of our First Follow-Up Audit are discussed in the **OC Internal Auditor's Report** following this transmittal letter. Our First Follow-Up Audit found that the Auditor-Controller has **partially implemented three (3) recommendations** from our original audit report.

A Second Follow-Up Audit will be conducted approximately six months from the date of this report on the three (3) remaining recommendations.

Each month I submit an **Audit Status Report** to the BOS where I detail any material 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 audit will be included in a future status report to the BOS.

Other recipients of this report are listed on the **OC Internal Auditor's Report** on page 4.

Table of Contents

First Follow-Up Access Request Application (ARA) Audit Using Computer-Assisted Audit Techniques (CAATs): Auditor-Controller Audit No. 1357-F1

As of April 22, 2015

OC Internal Auditor's Report

Audit No. 1357-F1 **July 31, 2015**

TO: Eric Woolery, CPA
Auditor-Controller

FROM: Dr. Peter Hughes, CPA, Director
Internal Audit Department

SUBJECT: First Follow-Up Audit - Access Request Application (ARA) Audit Using Computer-Assisted Audit Techniques (CAATs): Auditor-Controller, Original Audit No. 1357 Issued August 20, 2014

Scope of Review

We have completed a First Follow-Up Audit of Access Request Application (ARA) Audit Using Computer-Assisted Audit Techniques (CAATs). Our audit was limited to reviewing actions taken as of April 22, 2015, to implement **three (3) recommendations** from our original audit.

Background

At the time of our original audit, the process for requesting access to CAPS+ Financial/Purchasing, HR/Payroll and related systems (e.g., ERMI, VTI, and Personnel Data Warehouse) was a paper-based process known as **Access Request Form (ARF)**. All of these systems contain sensitive and/or critical data related to the County's financial, human resources and payroll information. During the original audit, the Auditor-Controller was in process of replacing ARF with **Access Request Application (ARA)**, which automates and streamlines the paper-based ARF process. Our original audit reviewed selected aspects of **ARA pre-implementation**. We utilized CAATs to identify existing security and workflow conflicts that potentially indicate that duties are not segregated and role conflicts exist. An important internal control component is the proper assignment and segregation of employee duties. **Segregation of duties** reduces the risk of both erroneous and improper actions. Roles and responsibilities are set up to **require at least two different people to view each transaction**.

Benefits of ARA include an automated "workflow" to help users find their ARA in the approval process; up-front segregation of duties (role conflict) validation, and an ability to copy existing user profiles. Security and workflow will be established that will require user ID and passwords; security roles, workflow rules and various levels of approval. ARA for CAPS+ Financial/Purchasing went live in October 2014 and went live for CAPS+ HR/Payroll in February 2015.

When using CAATs, often there is additional research needed to validate exceptions that is only known at the department level. Internal Audit attempts to validate and resolve exceptions; however, most of the resulting exceptions are forwarded to the appropriate department for validation and/or resolution. Depending on the department's review, **the exceptions may or may not be a finding**. For the exceptions and findings noted in this report, we forwarded the exceptions to the **Auditor-Controller Information Technology (Security & Workflow)**, for further research and/or clarifying existing CAPS+ access policies and procedures. In this report, we keep the details of our exceptions to a general discussion and do not identify specific user access. The Auditor-Controller has been provided with the specific details so they can conduct their research on the exceptions.

The original audit identified **three (3) Control Findings** to research and validate the reported exceptions and take corrective actions as deemed necessary.

Results

Our First Follow-Up Audit indicated Auditor-Controller **partially implemented the three (3) recommendations**. Based on our First Follow-Up Audit, the following is the implementation status of the three (3) original recommendations:

1. **Security and Workflow Policy Conflicts** **(Control Finding)**
   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: **Partially implemented.** Our original audit reviewed CAPS+ user accounts for potential security and workflow role conflicts as defined by the Auditor-Controller. Access Request Application (ARA) went live in October 2014 for Financial/Purchasing access requests and February 2015 for HR/Payroll access requests. ARA provides real time visibility to conflicts, and requires users to acknowledge the conflict and provide justification as to why they need the conflicting roles. Access requests containing conflicts are automatically routed to A-C Internal Audit for review/approval. The conflicts noted under this recommendation are from segregation of duty conflicts identified using the Auditor-Controller Internal Control Advisory Workgroup conflict matrices.

   Our First Follow-Up Audit found the Auditor-Controller Internal Control Advisory Workgroup came to a tentative agreement on revising the rules/guidelines that dictate the Segregation of Duties matrix in late 2014. Soon after, the interim Auditor-Controller was replaced by the newly elected Auditor/Controller. The Internal Control Advisory Workgroup is still planning on discussing this subject with the new Auditor-Controller.

   Internal Audit modified its CAAT routine based on the revised conflict matrices and account lock feature and noted the following:

   a. Financial/Purchasing Conflicts: Our CAAT analysis identified 93 conflicts (previously identified 106) as defined by CAPS+ Financial/Purchasing Conflicting Roles Table.
   b. HR/Payroll Conflicts: 460 conflicts (previously identified 870) as defined by CAPS+ Human Resources/Payroll Conflicting Roles Table

   Although the implemented processes has reduced the number of individuals with conflicting roles, there are conflicting roles that still need to be addressed. Because the Auditor-Controller has made progress in reducing the number of role conflicts, but still needs to address the remaining conflicts, we consider this recommendation as partially implemented.

   Planned Action: Auditor-Controller plans to come to an agreement on the rules used to govern the Segregation of Duties matrix by August 30, 2015. The matrix will be updated using those rules in early FY15-16, followed by outreach to users with conflicting roles, and asking them to submit revised access requests. For now, conflicts will continue to be monitored and analyzed as they appear on access requests in ARA.

2. **CAPS+ User Account Exceptions to HR Employee Records** **(Control Finding)**
   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: **Partially Implemented.** Our original audit compared CAPS+ user accounts with HR employee files to identify inactive employees, non-county employees and account names not conforming to standard naming conventions.

Our First Follow-Up Audit found that on a daily basis, ARA automatically locks the CAPS+ accounts of users who have separated from the County. Users with the "Delete User" role are notified when there are Separated or Transferred users in their Department. Those users can then initiate a delete user request which will go through workflow for approval. However, the Separation & Transfer process is dependent upon HR staff updating the employee status information in CAPS+ HR. There can be up to a two week delay with that information being entered into CAPS+.

Internal Audit modified its CAATs based on the revised conflict matrices and account lock feature and noted the following:

a. Non-County Employee Access: 149 (185 previously identified) CAPS+ user accounts not matched to an active employee.
b. Non-Active Employee Access: 70 (109 previously identified) CAPS+ user accounts matched to an employee record with a status other than "active."
c. Non-Standard Account: 12 (15 previously identified) CAPS+ user accounts (7 belong to system processes) that did not conform to the standard naming convention

We were informed that Non-County employee access (e.g., Superior Court, Special District employees) still needs to be addressed. The Auditor-Controller through its Internal Control Advisory Workgroup needs to develop policy and procedures to ensure these individuals' access is appropriate and is kept current. Non-Active employee access will continue to exist due employee turnover, promotions, transfers, terminations, etc. due to timing differences of data entry into CAPS+. The Auditor-Controller needs to coordinate with HR to make the separation and transfer data entry a priority. Non-Standard Accounts are a maintenance issue that does not impact effectiveness of CAPS+ security.

Although the implemented processes has reduced the number of exceptions, there are the above issues that still need to be addressed. Because the Auditor-Controller has made progress in reducing the number of exceptions, but still needs to address the remaining issues, we consider this recommendation as partially implemented.

Planned Action: Auditor-Controller will work on a process to obtain more timely information related to the appropriateness of system access for non-County users. Auditor-Controller will also work with CEO Human Resources to make the data entry of separation and transfer information into CAPS+ HR a higher priority.

3. CAPS+ Security Table Configuration (Control Finding)

The Auditor-Controller should research the reported exceptions and remove any unnecessary items.

Current Status: **Partially Implemented.** Our original audit reviewed CAPS+ security tables to identify issues in security roles, workflow roles, and CAPS+ resources. The exceptions found appeared to be maintenance issues that do not impact the effectiveness of the ARA application security.

Our First Follow-Up Audit found the CAPS+ HR/Payroll Conflicting Roles Table was updated to remove Inquiry/ERMI roles from any conflicts as they do not allow the types of access that must be segregated (Custody, Authorization, Recording, Reconciliation). That revised table is being used in the ARA system for the automated conflicting roles validation.

Internal Audit CAATs reviewed the CAPS+ security tables for inconsistencies and noted the following:

a. 261 Security roles do not grant access to CAPS+ resources (172 previously identified).
b. 115 Security roles not associated with a user (76 previously identified).
c. 121 Workflow roles not associated with a user (73 previously identified).
d. 66 Workflow roles do not grant access to CAPS+ documents (58 previously identified).
e. 78 Workflow roles granting access to CAPS+ documents not defined in the workflow table (6 previously identified).
f. 91 CAPS+ resources not associated with a security role (31 previously identified).

These items are the result of using the CAPS+ security tables to document assignment of roles and responsibilities performed outside of the application (e.g., check pick up, invoice receiver). Although these items do not affect the effectiveness of the application security, it may cause efficiency issues (unnecessary security table entries). Because the list of valid exceptions has been started, but needs to be completed, we consider this recommendation as partially implemented.

Planned Action: Auditor-Controller plans to complete the list of valid exceptions by August 30, 2015.

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 834-5475 or Michael Goodwin, Assistant Director at 834-6066.

Distribution Pursuant to Audit Oversight Committee Procedure No. 1:

Members, Board of Supervisors
Members, Audit Oversight Committee
Frank Kim, Chief Executive Officer
Mark Denny, Chief Operating Officer
Phil Daigneau, Director, Information Technology
Bill Malohn, Manager, CAPS+ Security
Claire Moynihan, Director, A-C Operations
Foreperson, Grand Jury
Robin Stieler, Interim Clerk of the Board of Supervisors
Macias, Gini & O'Connell, LLP, County External Auditor