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'
OC 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

Transmittal Letter	**i**
OC Internal Auditor's Report	**1**

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

AUDIT OF ACCESS REQUEST APPLICATION (ARA) USING COMPUTER-ASSISTED AUDIT TECHNIQUES (CAATS): AUDITOR-CONTROLLER

(Cited as a Best Practice by the Institute of Internal Auditors)

As of May 31, 2014

The Auditor-Controller is implementing an automated workflow process to replace the existing paper based process for authorizing access to the CAPS+ system resources and assigning user security roles. We reviewed design documentation for the automated Access Request Application (ARA) to identify controls that if implemented properly would facilitate appropriate segregation of duties, reviews and approvals, audit trails, and reconciliations. We also analyzed 2,571 CAPS+ user accounts as of November 1, 2013, to identify potential segregation of duties conflicts, inappropriate user access, and CAPS+ security table issues.

Our CAAT routines identified several exceptions that require further research by the Auditor-Controller to determine whether an exception existed. We identified three (3) Control Findings for the Auditor-Controller to perform further research on the reported findings to determine if they are valid exceptions.

AUDIT NO: 1357
REPORT DATE: AUGUST 20, 2014

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

(*Certified Information System Auditor)

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 J. Goodwin **CPA, CIA**
Senior Audit Manager

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

Hall of Finance & Records

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

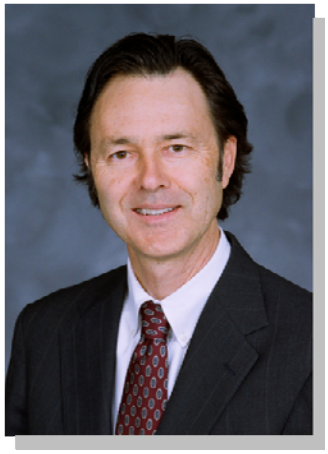
Phone: (714) 834-5475 Fax: (714) 834-2880

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 **August 20, 2014**

TO: Jan E. Grimes, CPA
Auditor-Controller

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

SUBJECT: Audit of Access Request Application (ARA) Using Computer-Assisted Audit Techniques (CAATs): Auditor-Controller

We have completed an Audit of Access Request Application (ARA) Using Computer-Assisted Audit Techniques (CAATs) as of May 31, 2014. We performed this audit in accordance with our *FY 2013-14 Audit Plan and Risk Assessment* approved by the Audit Oversight Committee and the Board of Supervisors. The final report is attached for your information.

Please note we have a structured and rigorous **Follow-Up Audit** process in response to recommendations and suggestions made by the Audit Oversight Committee (AOC) and the Board of Supervisors (BOS). Our **First Follow-Up Audit** will begin at six months from the official release of the report. A copy of all our Follow-Up Audit reports is provided to the BOS as well as to all those individuals indicated on our standard routing distribution list.

The AOC and BOS expect that audit recommendations will typically be implemented within six months and often sooner for significant and higher risk issues. Our **Second Follow-Up Audit** will begin at six months from the release of the first Follow-Up Audit report, by which time **all** audit recommendations are expected to be addressed and implemented. At the request of the AOC, we are to bring to their attention any audit recommendations we find still not implemented or mitigated after the second Follow-Up Audit. The AOC requests that such open issues appear on the agenda at their next scheduled meeting for discussion.

Each month I submit an **Audit Status Report** to the BOS where I detail any material and significant audit issues 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.

As always, the Internal Audit Department is available to partner with your staff so that they can successfully implement or mitigate difficult audit recommendations. Please feel free to call me should you wish to discuss any aspect of our audit report or recommendations. Additionally, we will request your department complete a **Customer Survey** of Audit Services. You will receive the survey shortly after the distribution of our final report.

ATTACHMENTS

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

Table of Contents

Audit of Access Request Application (ARA) Using Computer-Assisted Audit Techniques (CAATs): Auditor-Controller
Audit No. 1357

As of May 31, 2014

Transmittal Letter i

OC Internal Auditor's Report

- **OBJECTIVES** 1
- **RESULTS** 2
- **BACKGROUND** 3
- **SCOPE** 3

Detailed Results, Findings, Recommendations and Management Responses

Finding 1 – Security and Workflow Policy Conflicts (Control Finding) 6

Finding 2 – CAPS+ User Account Exceptions to HR Employee Records (Control Finding) 6

Finding 3 – CAPS+ Security Table Configuration (Control Finding) 7

ATTACHMENT A: Report Item Classifications 8

ATTACHMENT B: Auditor-Controller Management Responses 9

OC Internal Auditor's Report

Audit No. 1357 **August 20, 2014**

TO: Jan E. Grimes, CPA
Auditor-Controller

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

SUBJECT: Audit of Access Request Application (ARA) Using Computer-Assisted Audit Techniques (CAATs): Auditor-Controller

Audit Highlight

We reviewed ARA design documentation to identify application controls if implemented properly would facilitate appropriate segregation of duties, reviews and approvals, audit trails, and reconciliations.

We also analyzed 2,571 CAPS+ user accounts as of November 1, 2013, to identify potential segregation of duties conflicts, inappropriate CAPS+ user access, and CAPS+ security table issues.

We identified three **(3) Controls Findings** that require action by the A-C to resolve CAPS+ policy conflicts, unnecessary CAPS+ access, and unnecessary security table entries.

OBJECTIVES

In accordance with our *FY 2013-2014 Audit Plan and Risk Assessment* approved by the Audit Oversight Committee and Board of Supervisors, the Internal Audit Department conducted an audit of Access Request Application (ARA). We reviewed design documentation for ARA as well as performed a variety of audit tests of CAPS+ user access records utilizing Computer-Assisted Audit Techniques (known by the acronym CAATs). This audit was conducted in conformance with the Professional Practice of Internal Auditing prescribed by the Institute of Internal Auditors.

Our objective was to review design documentation to identify controls that if implemented properly would facilitate appropriate segregation of duties, reviews and approvals, audit trails, and reconciliations. In addition, we analyzed CAPS+ user access tables to determine whether the CAPS+ user accounts as established provided an adequate segregation of duties. To accomplish this, we performed the following objectives:

1. **Reviewed ARA design documents to identify application controls:** Reviewed documentation to identify application controls that if implemented properly would facilitate:
   - Appropriate segregation of duties,
   - Reviews and approvals,
   - Audit trails, and
   - Reconciliations.

2. **Analyzed CAPS+ User Access to identify policy conflicts:** Reviewed CAPS+ user accounts for potential security and workflow role conflicts as defined by Auditor-Controller.

3. **Compared CAPS+ User Accounts with HR employee files to identify inappropriate access:** Compared CAPS+ user accounts with HR employee file to identify:
   - Inactive employees,
   - Non county employees, and
   - Account names not conforming to standard.

4. **Analyzed CAPS+ Security Tables to identify inefficiencies:** Reviewed CAPS+ security tables to identify issues in the following areas:
   - Security roles,
   - Workflow roles, and
   - CAPS+ resources.

RESULTS

Objective #1 – ARA Application Controls:

We reviewed ARA design documentation to identify application controls in the areas of: segregation of duties, reviews and approvals, audit trails, and reconciliations and found adequate controls in the written documents. Based on our review of design documentation, we determined that the application controls identified, **if implemented properly**, would facilitate appropriate segregation of duties, reviews and approvals, audit trails, and reconciliations.

We have no findings or recommendations under this objective.

Objective #2 – Security and Workflow Policy Conflicts:

We used a CAAT routine to identify potential segregation of duties issues based on the Auditor-Controller's defined security role conflicts for both the Financial/Purchasing and HR/Payroll systems. The Auditor-Controller had identified 270 Financial/Purchasing role conflicts and 12 HR/Payroll role conflicts.

Our CAAT analysis performed on 2,571 CAPS+ user accounts identified the following:

- 106 Financial/Purchasing conflicts relating to 61 user accounts, and
- 870 HR/Payroll conflicts relating to 122 user accounts.

We identified **one (1) Control Finding** to implement ARA and resolve the CAPS+ user conflicts. (See the *Detailed Results, Findings, Recommendations and Management Responses* section of this report.)

Objective #3 – Comparison to HR Employee Records:

We compared the CAPS+ user accounts with the HR employee data file as of November 1, 2013, to identify non-County user access and separated employees. Our CAAT analysis performed on 2,571 CAPS+ user accounts identified the following:

- 185 (47 belong to special districts, courts) CAPS+ user accounts not matched to an active employee;
- 109 CAPS+ user accounts matched to an employee record with a status other than active; and
- 15 CAPS+ user accounts (12 related to system processes) that did not conform to the standard naming convention.

We identified **one (1) Control Finding** to resolve the CAPS+ user access issues.

Objective #4 – CAPS+ Security Tables:

We analyzed the CAPS+ security tables including security role tables, workflow role tables, and resource definition tables to identify potential issues and identified the following:

- 31 CAPS+ resources not associated with a security role,
- 172 Security roles that do not grant access to CAPS+ resources,
- 76 Security roles not associated with a user,
- 73 Workflow roles not associated with a user,
- 58 Workflow roles that do not grant access to CAPS+ documents, and
- 6 Workflow roles granting access to CAPS+ documents not defined in the workflow table.

We identified **one (1) Control Finding** to perform further research and resolve these issues.

BACKGROUND

The current process for requesting access to CAPS+ Financial/Purchasing, HR/Payroll and related systems (e.g., ERMI, VTI, and Personnel Data Warehouse) is a paper-based process. All of these systems contain sensitive and/or critical data related to the County's financial, human resources and payroll information. Currently, a paper **Access Request Form (ARF)** is used that must be signed and routed to various approvers for a wet signature. The ARF is designed to ensure the creation and approval of transactions (financial, budget, purchasing, payroll, human resources) is performed only by authorized users. 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**.

The **ARA (Access Request Application)** automates the paper-based process and will streamline the current ARF process. 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. The ARA system was intended to go-live in June 2014, but was postponed to September 2014.

Our audit reviewed selected aspects of **pre-implementation** of ARA. We utilized CAATs to identify existing security and workflow conflicts (indicating that duties are not segregated). CAATs differ from our traditional audits in that CAATs can query **100%** of a data universe whereas the traditional audits typically test but a **sample** of transactions from the population. CAATs are automated queries applied to large amounts of electronic data searching for specified characteristics. We use a proprietary, best practice and industry recognized software product (ACL) to help us in this process.

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 preliminary exceptions to the **Auditor-Controller (A-C)** on December 18, 2013, for further research and/or clarifying existing CAPS+ access policies and procedures. In this report, we are keeping the details of our exceptions to a general discussion and do not identify specific user access. The A-C has been provided with the specific details of user access so they can conduct their research on the exceptions.

SCOPE

Our scope was conducting a CAAT analysis on 2,571 CAPS+ user accounts as of November 1, 2013, and included the following documents: *ARA Scope of Work, ARA Testing Instructions, Instructional Aide, & Test Scripts/Cases, ARF Automation Design, Security & Workflow Design*, and *CAPS+ Security Tables*. Our analysis included a review in the following areas:

1. **ARA Design Documentation:** We reviewed the ARA design documentation for controls in the following areas: segregation of duties, reviews and approvals, audit trails, and reconciliations.

2. **Security and Workflow Policy Conflicts:** We analyzed 2,571 CAPS+ user accounts for segregation of duties conflicts as defined by the A-C CAPS+ Conflicting Roles Tables.

3. **Comparison to HR Employee Records:** We compared all 2,571 CAPS+ user accounts with the Human Resources employee data file to identify user account issues.

4. **CAPS+ Security Tables:** We analyzed the CAPS+ security tables including security roles, workflow roles, and resources tables to identify potential issues.

OC Internal Auditor's Report

To accomplish the above, we worked with **Auditor-Controller/Information Technology** and **Auditor-Controller/Internal Audit**. The Auditor-Controller/Information Technology managers over CAPS+ Financial/Purchasing and HR/Payroll assisted us in researching our exceptions and helping refine our CAAT routines used in the audit.

Acknowledgment

We appreciate the courtesy extended to us by the Auditor-Controller personnel during our audit. If we can be of further assistance, please contact me directly at 834-5475 or Michael Goodwin, Senior Audit Manager, at 834-6066.

Attachments

Distribution Pursuant to Audit Oversight Committee Procedure No. 1:

Members, Board of Supervisors
Members, Audit Oversight Committee
Michael Giancola, County Executive Officer
Frank Kim, Chief Financial Officer
Mark Denny, Chief Operating Officer
Denise Steckler, Chief Deputy Auditor-Controller
Victoria Ross, Director, Central Accounting Operations, Auditor-Controller
Phil Daigneau, Director, Information Technology, Auditor-Controller
Bill Malohn, Manager, CAPS+ Financial/Purchasing, Auditor-Controller
Teresa White, Manager, CAPS+ HR/Payroll, Auditor-Controller
Foreperson, Grand Jury
Susan Novak, Clerk of the Board of Supervisors
Macias Gini & O'Connell LLP, County External Auditor

Detailed Results, Findings, Recommendations and Management Responses

1. ARA Design Documentation (Objective #1)

We reviewed design documentation for the ARA application including: *ARA Scope of Work, ARF Automation Design, Security and Workflow Design, and ARA Testing Instructions, Instructional Aide & Test Scripts/Cases* and identified the following application controls:

- **Segregation of Duties**
  - ARA will automate the processing of CAPS+ access requests including a workflow feature (email notifications and documented approvals) that will allow users to monitor progress of their access request from initial request through final approval.
  - ARA will prevent segregation of duties conflicts as defined in the policy.
  - ARA security roles will limit user's capabilities similar to ERMI where access to confidential documents (such as access request form) is restricted.
  - An ARA administrator account will be established to configure/edit ARA including: procedures for assignment/use/deactivation of the ARA administrator account; audit logs of account activity; and email notifications to a pre-determined distribution list.

- **Review and Approval**
  - ARA will automate the processing of CAPS+ access requests including a workflow feature (email notifications and documented approvals) that will allow users to monitor progress of their access request from initial request through final approval.

- **Audit Trails**
  - ARA will have an audit trail of all activity within system.

- **Reconciliation**
  - ARA will allow provide reconciliation reports between ARA and CAPS+.

- **Other Security Features**
  - ARA password criteria is configurable. For the ARA testing phase, password settings were simplified: 4 characters including numeric, upper case, and lower case with the last 3 passwords in history. For production, the password settings will be strengthened: 8 characters including numeric, upper case, and lower case with the last 3 passwords in history.
  - ARA will enable control of user email accounts, which is a key field in the administration of user accounts.
  - ARA has automatic locking accounts for users that have been separated or transferred when processed by CAPS+ HR.

Conclusion:

Based on our limited review of design documentation, we determined that the application controls identified, **if implemented properly**, would facilitate appropriate segregation of duties, reviews and approvals, audit trails, and reconciliations. **No findings were noted under this objective.**

2. Security and Workflow Policy Conflicts (Objective #2)

We used a CAAT routine to identify potential segregation of duties issues based on Auditor-Controller defined security role conflicts for both the Financial and HR/Payroll systems. The Auditor-Controller had identified 270 Financial/Purchasing conflicts and 12 HR/Payroll conflicts.

Detailed Results, Findings, Recommendations and Management Responses

Conclusion:
This analysis was intended to identify exceptions that require further research to determine if they are indicative of a CAPS+ segregation of duties issue. We forwarded these exceptions to the Auditor-Controller for research and resolution, and were informed that these items would be resolved with the implementation of ARA. As such, we identified **one (1) Control Finding** to implement ARA and resolve the CAPS+ user conflicts:

Finding 1 – Security and Workflow Policy Conflicts (Control Finding)

a. Financial/Purchasing Conflicts: Our CAAT analysis identified 106 conflicts (assigned to 61 user accounts) as defined by CAPS+ Financial/Purchasing Conflicting Roles Table.
b. HR/Payroll Conflicts: 870 conflicts (assigned to 122 user accounts) as defined by CAPS+ Human Resources/Payroll Conflicting Roles Table.

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.

Auditor-Controller Management Response:
Concur. Auditor-Controller plans to implement the Access Request Application (ARA) in September 2014. The use of this new system will limit future conflicts from occurring within CAPS+. Each time a County User requests access to the various CAPS+ systems, ARA will systematically compare requested Security Roles against established Conflicting Roles Matrices. This function can be configured to require an additional workflow step to review the specific conflicts or to prevent the conflicts all together.

In fiscal year 2014-2015, the Auditor-Controller Internal Control Advisory Workgroup will review and revise the existing CAPS+ Conflicting Roles Matrices. After the matrices have been revised, they will be loaded in ARA. Once the Conflicting Roles Matrices are revised, the CAPS+ Security Team will contact users to resolve any remaining conflicts. This will involve the users submitting revised access requests through the ARA system to eliminate conflicts.

3. Comparison to HR Employee Records (Objective #3)

We compared the 2,571 CAPS+ User Accounts with the Human Resources employee records to identify CAPS+ user access issues. This analysis was intended to identify exceptions that require further research to determine if they are indicative of a CAPS+ user access concern.

Conclusion:
Based on our analysis of the CAPS+ user accounts and the Auditor-Controller's preliminary research of the exceptions, we were informed that these issues will be addressed with the implementation of ARA. As such, we identified **one (1) Control Finding** to implement ARA and resolve the CAPS+ user access issues.

Finding 2 - CAPS+ User Account Exceptions to HR Employee Records (Control Finding)

a. Non-County Employee Access: 185 (47 belong to special districts, courts) CAPS+ user accounts not matched to an active employee.
b. Non-Active Employee Access: 109 CAPS+ user accounts matched to an employee record with a status other than "active."
c. Non-Standard Account: 15 CAPS+ user accounts (12 belong to system processes) that did not conform to the standard naming convention.

Detailed Results, Findings, Recommendations and Management Responses

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.

Auditor-Controller Management Response:
Concur. Auditor-Controller plans to implement ARA in September 2014. This application includes a "Separations and Transfers" feature which will reduce the number of CAPS+ User Account Exceptions to HR Employee Records. On a nightly basis, ARA will examine each user's HR status to determine whether they are in a "separated" or "transferred" state. If a user has separated from the County, their accounts will be locked and department representatives will be notified to delete the user's access. If the user has transferred, their situation will be reviewed by the CAPS+ Security Team to determine the proper disposition. ARA will also have aging feature that will generate notifications to each department should they have users who no longer require access.

4. CAPS+ Security Tables (Objective #4)
We reviewed CAPS+ security tables for issues. This analysis was intended to identify exceptions that require further research to determine if they are indicative of a CAPS+ user access concern.

Conclusion:
Based on our analysis and the Auditor-Controller's preliminary research of the exceptions, we were informed that the majority of these items relate to either notifications (emails) or documentation (document who is performing manual processes) items and the other items are maintenance issues that will be resolved when ARA is implemented. As such, we identified **one (1) Control Finding** to perform further research and resolve these issues.

Finding 3 - CAPS+ Security Table Configuration (Control Finding)

a. 172 Security roles that do not grant access to CAPS+ resources.
b. 76 Security roles not associated with a user.
c. 73 Workflow roles not associated with a user.
d. 58 Workflow roles that do not grant access to CAPS+ documents.
e. 6 Workflow roles granting access to CAPS+ documents not defined in the workflow table.
f. 31 CAPS+ resources not associated with a security role.

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

Auditor-Controller Management Response:
Concur. Auditor-Controller will create and maintain a list of valid exceptions, which will contain the names of roles/resources and an explanation of why they are valid. The majority of the exceptions noted in the audit finding are valid (i.e. ERMI roles, non-approval workflow notifications, etc.).

Auditor-Controller will review the roles/resources and remove any that are unnecessary by December 2014.

Detailed Results, Findings, Recommendations and Management Responses

ATTACHMENT A: Report Item Classifications

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

- **Critical Control Weaknesses:**
  Audit findings or a combination of Significant Control Weaknesses that represent serious exceptions to the audit objective(s), policy and/or business goals. Management is expected to address Critical Control Weaknesses brought to their attention immediately.

- **Significant Control Weaknesses:**
  Audit findings or a combination of Control Findings that represent a significant deficiency in the design or operation of internal controls. Significant Control Weaknesses require prompt corrective actions.

- **Control Findings:**
  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.

Detailed Results, Findings, Recommendations and Management Responses

ATTACHMENT B: Auditor-Controller Management Responses

ORANGE COUNTY AUDITOR-CONTROLLER

HALL OF RECORDS
12 CIVIC CENTER PLAZA, ROOM 200
POST OFFICE BOX 567
SANTA ANA, CALIFORNIA 92702-0567

(714) 834-2450 FAX: (714) 834-2569
www.ac.ocgov.com

JAN E. GRIMES, CPA
AUDITOR-CONTROLLER

DENISE STECKLER
CHIEF OF STAFF

TONYA BURNETT, CPA
CHIEF DEPUTY AUDITOR-CONTROLLER
SATELLITE ACCOUNTING OPERATIONS

PHILLIP T. DAIGNEAU
CHIEF DEPUTY AUDITOR-CONTROLLER
INFORMATION TECHNOLOGY

FRANK DAVIES, CPA
CHIEF DEPUTY AUDITOR-CONTROLLER
PROPERTY TAX

VICTORIA ROSS, CPA
CHIEF DEPUTY AUDITOR-CONTROLLER
CENTRAL ACCOUNTING OPERATIONS

August 15, 2014

TO: Peter Hughes, Director
Internal Audit Department

ATTN: Alan Marcum, Senior Audit Manager

SUBJECT: Audit Report No. 1357 – Audit of Access Request Application (ARA) Using Computer-Assisted Audit Techniques (CAATs)

Following is our response to the recommendations contained in the report on 1357 – Audit of Access Request Application (ARA), Using Computer-Assisted Audit Techniques (CAATs) – Audit Report No. 1357.

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.

Auditor-Controller Response

Concur: Auditor-Controller plans to implement the Access Request Application (ARA) in September 2014. The use of this new system will limit future conflicts from occurring within CAPS+. Each time a County User requests access to the various CAPS+ systems, ARA will systematically compare requested Security Roles against established Conflicting Roles Matrices. This function can be configured to require an additional workflow step to review the specific conflicts or to prevent the conflicts all together.

In fiscal year 2014-2015, the Auditor-Controller Internal Control Advisory Workgroup will review and revise the existing CAPS+ Conflicting Roles Matrices. After the matrices have been revised, they will be loaded into ARA. Once the Conflicting Roles Matrices are revised, the CAPS+ Security Team will contact users to resolve any remaining conflicts. This will involve the users submitting revised access requests through the ARA system to eliminate conflicts.

Detailed Results, Findings, Recommendations and Management Responses

ATTACHMENT B: Auditor-Controller Management Responses

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.

Auditor-Controller Response

Concur: Auditor-Controller plans to implement ARA in September 2014. This application includes a "Separations and Transfers" feature which will reduce the number of CAPS+ User Account Exceptions to HR Employee Records. On a nightly basis, ARA will examine each user's HR status to determine whether they are in a "separated" or "transferred" state. If a user has separated from the County, their accounts will be locked and department representatives will be notified to delete the user's access. If a user has transferred, their situation will be reviewed by the CAPS+ Security Team to determine the proper disposition. ARA will also have an aging feature that will generate notifications to each department should they have users who no longer require access.

Recommendation No. 3

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

Auditor-Controller Response

Concur: Auditor-Controller will create and maintain a list of valid exceptions, which will contain the names of roles/resources and an explanation of why they are valid. The majority of the exceptions noted in the audit finding are valid (i.e. ERMI roles, non-approval workflow notifications, etc.).

Auditor-Controller will review the roles/resources and remove any that are unnecessary by December 2014.

for Jan E. Grimes
Auditor-Controller

wg\audit rsp 1357