FIRST FOLLOW-UP AUDIT

INFORMATION TECHNOLOGY AUDIT:
CAPS STEERING COMMITTEE
CAPS+ FINANCIAL SYSTEM
ORACLE DATABASE CONFIGURATION

ORIGINAL AUDIT NO. 2948

AS OF JUNE 23, 2011

Our First Follow-Up Audit found that the CAPS Steering Committee (supported by the Auditor-Controller and CEO/Information Technology) fully implemented nine (9) recommendations and one (1) recommendation is in process from our original audit report dated October 27, 2010.

AUDIT NO: 1050-B
REPORT DATE: JULY 14, 2011

Director: Dr. Peter Hughes, Ph.D., CPA
Deputy Director: Eli Littner, CPA, CIA
Senior IT Audit Manager: Autumn McKinney, CPA, CIA, CISA
IT Audit Manager: Wilson Crider, CPA, CISA

Independence Objectivity Integrity

OC Internal Audit Department

ORANGE COUNTY BOARD OF SUPERVISORS'

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

Providing Facts and Perspectives Countywide

RISK BASED AUDITING

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

Eli Littner — **CPA, CIA, CFE, CFS, CISA**
Deputy Director
Certified Fraud Specialist (CFS)
Certified Information Systems Auditor (CISA)

Michael Goodwin — **CPA, CIA**
Senior Audit Manager

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

Autumn McKinney — **CPA, CIA, CISA, CGFM**
Senior Audit Manager
Certified Government Financial 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

Orange County's Internal Audit — Fraud Hot-Line — 24/7 Fraud Hotline

OC Fraud Hotline (714) 834-3608

Letter from Dr. Peter Hughes, CPA

Transmittal Letter

Audit No. 1050-B **July 14, 2011**

TO: CAPS Steering Committee
David Sundstrom, Auditor-Controller, Chair
Bob Franz, Chief Financial Officer, Vice Chair
Mahesh Patel, Acting Deputy CEO/CIO
Carl Crown, Human Resources Director
Shaun Skelly, Chief Deputy Auditor-Controller

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

SUBJECT: First Follow-Up Audit: CAPS+ Financial System - Oracle Database Configuration, Original Audit No. 2948, Issued October 27, 2010

We have completed a First Follow-Up Audit of the CAPS+ Financial System - Oracle Database Configuration. Our audit was limited to reviewing, as of June 23, 2011, actions taken to implement the **ten (10) recommendations** from our original audit. We conducted this First Follow-Up Audit in accordance with the *FY 10-11 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 the CAPS Steering Committee **fully implemented nine (9) recommendations and one (1) recommendation is in process**.

Each month I submit an **Audit Status Report** to the BOS where I detail any critical and significant control weaknesses 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 Audit of Information Technology Audit:
CAPS Steering Committee
CAPS+ Financial System - Oracle Database Configuration
Audit No. 1050-B

As of June 23, 2011

OC Internal Auditor's Report

Audit No. 1050-B **July 14, 2011**

TO: CAPS Steering Committee
David Sundstrom, Auditor-Controller, Chair
Bob Franz, Chief Financial Officer, Vice-Chair
Mahesh Patel, Acting Deputy CEO/CIO
Carl Crown, Human Resources Director
Shaun Skelly, Chief Deputy Auditor-Controller

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

SUBJECT: First Follow-Up Audit of CAPS+ Financial System - Oracle Database Configuration, Original Audit No. 2948, Issued October 27, 2010.

Scope of Review

We have completed a First Follow-Up Audit of the CAPS+ Financial System - Oracle Database Configuration. Our audit was limited to reviewing actions taken as of June 23, 2011 to implement the **ten (10) recommendations** made in our original audit report.

Background

The original audit reviewed the Oracle database to determine whether it was configured to secure the CAPS+ financial system data. The audit included a review of the Oracle database configurations (settings) in the following areas:

- Account Profiles: database account characteristics including password and database resource management settings;
- Privileges and Authorizations: database account capabilities;
- Listener: service providing connectivity to the database;
- Data Security: protection of confidential data (taxpayer ID, bank account data) stored in the database;
- Operating System: operating system file and directory permissions to Oracle database system and data files;
- Database Links: providing access to database data;
- Auditing/Logging: capturing database activity (i.e., database logon attempts, system account activity, etc.) to effectively monitor the database;
- Authentication: verifying user access to the database;
- Database Parameter Settings: reviewing Oracle configuration files including init.ora, sqlnet.ora and tnsnames.ora to ensure they are sufficiently configured; and
- Other Related Oracle Database Security Features: Oracle provides security features in addition to its core database software including: Oracle Wallet Manager, SSL Authentication, Virtual Private Database and Oracle Database Vault.

The original audit identified one (1) **significant issue** and nine (9) **control findings**. For the original audit, we issued both a public and confidential report (containing more details) due to the sensitivity of certain issues. Because those recommendations have now been fully implemented, a separate confidential follow-up audit report is not needed and there is only this public follow-up audit report issued.

Results

Our First Follow-Up Audit indicated the CAPS Steering Committee (supported by the Auditor-Controller and CEO/Information Technology) **fully implemented nine (9) recommendations and one (1) recommendation is in process.** We believe the remaining **one (1) recommendation** is still appropriate and further efforts should be made to fully implement it. Based on the Follow-Up Audit we conducted, the following is the implementation status of the ten (10) original recommendations.

1. **There is No Database Auditing/Logging Performed** **(Significant Issue)**
   We recommend that the CAPS Steering Committee ensure an auditing/logging strategy is developed and implemented for the CAPS+ Oracle database, including activating the "SYS" activity logging feature. Any sensitive/confidential tables (such as those containing vendor banking information) should be logged and their accesses reviewed for appropriateness.

   Current Status: **Fully Implemented.** Database auditing/logging has been implemented including "SYS" activity, specific privileges by users, and fine grain auditing for specific database objects (including vendor banking information). While we did not comprehensively evaluate the adequacy of items being logged and the related monitoring, we did perform a high-level review and the logging implemented appears reasonable. In addition, a monthly extract from the database audit trails is sent to Auditor-Controller/Information Technology (A-C/IT) and the CAPS+ Program Management Office (PMO) for their review. Therefore, we consider this recommendation fully implemented.

2. **Need to Establish Personal Accounts for DBAs** **(Control Finding)**
   We recommend that CEO/IT establish personal accounts for the database administrators to use when performing their duties whenever possible.

   Current Status: **Fully Implemented.** The database administrators (DBAs) now use their own individual user accounts to perform most of the administration activities. Any changes or activities requiring usage of the SYS account must be submitted, reviewed and approved as part of the CEO/IT standard request for change authorization form/process. In addition, the DBAs and SYS accounts activities are now logged (see recommendation 1 above) and the output provided monthly to A-C/IT and CAPS PMO. Therefore, we consider this recommendation fully implemented.

3. **Account Profile Password Settings Do Not Meet Best Practice** **(Control Finding)**
   No recommendation is needed as sufficient corrective action was quickly taken by CEO/IT after our fieldwork was completed.

   Current Status: **Fully Implemented** at time of original report issuance. Therefore, we consider this recommendation fully implemented.

4. **Password Verify Function Is Not Used** **(Control Finding)**
   No recommendation is needed as sufficient corrective action was quickly taken by CEO/IT after our fieldwork was completed.

   Current Status: **Fully Implemented** at time of original report issuance. Therefore, we consider this recommendation fully implemented.

5. **Account Profile Resource Settings Were Left as Default** (Control Finding)
No recommendation is needed as sufficient corrective action was quickly taken by CEO/IT after our fieldwork was completed.

Current Status: **Fully Implemented** at time of original report issuance. Therefore, we consider this recommendation fully implemented.

6. **Listener Configuration Settings Do Not Meet Best Practices** (Control Finding)
We recommend that CEO/IT activate the "Admin_restrictions" and modify the "inbound_connect_timeout" to best practices.

Current Status: **Fully Implemented.** Admin_restrictions parameter for the listener has been changed as suggested. After further research by CEO/IT (there are already connection timeout messages in the alert logs), it was decided to keep the current value of inbound_connect_timeout the same since changing the value would negatively impact the application's performance. This appears reasonable. Therefore, we consider this recommendation fully implemented.

7. **External Processes Functionality Is Allowed** (Control Finding)
We recommend that CEO/IT remove the external process configuration if the capability is not required by the CAPS+ financial system. If it is required, then CEO/IT should modify the configuration to properly secure it.

Current Status: **Fully Implemented.** External process configuration in the listener has been removed. Therefore, we consider this recommendation fully implemented.

8. **Unnecessary User "Read" Access Granted to the Oracle Database** (Control Finding)
We recommend that CEO/IT remove the unnecessary "Read" access to the Oracle database.

Current Status: **Fully Implemented.** The unnecessary "Read" access has been removed by CEO/IT based on the input provided by the Auditor-Controller. Additionally, A-C/IT reviews the monthly audit trail extracts (see recommendation 1 above) to help ensure the database access is kept current. Therefore, we consider this recommendation fully implemented.

9. **More Secure Command Is Not Utilized When Changing User Account Passwords** (Control Finding)
No recommendation is needed as sufficient corrective action was quickly taken by CEO/IT after our fieldwork was completed.

Current Status: **Fully Implemented** at time of original report issuance. Therefore, we consider this recommendation fully implemented.

10. Other Oracle Security Features Not Utilized (Control Finding)

We recommend that the CAPS Steering Committee ensure the above Oracle security features are researched and those features are implemented that do not conflict with the CAPS+ financial system and are cost effective. Highest priority should be given to implementing the Oracle Database Vault to prevent privileged users from modifying the CAPS+ financial system database outside of the CAPS+ application and its internal control structure. If the Oracle Database Vault is unable to be implemented, the auditing/logging recommendation proposed for Findings Nos. 1 and 2 above will be even more important to help detect any unauthorized changes made directly to the database table containing vendor banking information.

Current Status: **In Process.** CEO/IT performed a preliminary investigation, researched technology options, and consulted with Oracle's Oracle Enterprise Manager (OEM) for best practices. CEO/IT made technical recommendations via a memo to the CAPS PMO and A-C/IT. Pending the CAPS PMO decision, CEO/IT worked with AC/IT to implement new security roles to require a higher authorized user (i.e. DBA or super user) access (which is being controlled) to perform any changes to the production database outside the CAPS+ application.

Planned Action:
The CAPS PMO and CAPS Steering Committee reviewed the CEO/IT's initial research of the Oracle security features and requested additional information regarding the Oracle Database Vault product. Upon receipt of the additional information, the CAPS PMO and CAPS Steering Committee will review the options and determine which actions, if any, to undertake by October 2011.

We appreciate the assistance extended by the Auditor-Controller/Information Technology, CAPS Program Management Office, and CEO/Information Technology during our Follow-Up Audit. If you have any questions, please contact me directly or Eli Littner, Deputy Director at 834-5899, or Autumn McKinney, Senior IT Audit Manager at 834-6106.

Distribution Pursuant to Audit Oversight Committee Procedure No. 1:

Members, Board of Supervisors
Members, Audit Oversight Committee
Thomas G. Mauk, County Executive Officer
Joel Manfredo, Chief Technology Officer, CEO/Information Technology
Sreesha Rao, Director, Business Information Services, CEO/Information Technology
Sanjukta Chakraborty, CEO/Information Technology
Tony Lucich, Chief Security Officer, CEO/Information Technology
Phil Daigneau, Director, Auditor-Controller/Information Technology
Steve Rodermund, Manager, CAPS Program Management Office
Foreperson, Grand Jury
Darlene J. Bloom, Clerk of the Board of Supervisors