

Internal Audit Department

O R A N G E C O U N T Y
6th Largest County in the USA

PUBLIC REPORT

Information Technology Audit: CAPS STEERING COMMITTEE (CSC) CAPS+ FINANCIAL SYSTEM ORACLE DATABASE CONFIGURATION

As of January 31, 2010

Critical
Impact
Audit

RECORDS OVER \$3.4
BILLION COLLECTED &
DISBURSED ANNUALLY

We audited the Oracle database configuration (settings) used by the CAPS+ financial system. The County of Orange implemented CAPS+ on July 1, 2009 as its enterprise financial system to record general ledger, fixed asset, cost accounting, purchasing, cash receipting, and accounts payable transactions. The CAPS+ financial system uses Oracle 10g as its database management software. Although the CAPS+ financial system contains mainly non-confidential information, it does contain some sensitive or protected information.

We found that the Oracle database was generally configured to secure the CAPS+ financial system data, but there are enhancements that can and should be made to provide better security. We identified **one (1) Significant Issue** and **nine (9) Control Findings** to improve configurations, controls, and processes for the Oracle database. The CAPS Steering Committee and CEO/IT agreed with all ten (10) findings and recommendations.

AUDIT NO: 2948-A
REPORT DATE: OCTOBER 27, 2010

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

RISK BASED AUDITING

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



American Institute of Certified Public Accountants Award to Dr. Peter Hughes as 2010 Outstanding CPA of the Year for Local Government



2009 Association of Certified Fraud Examiners' Hubbard Award to Dr. Peter Hughes for the Most Outstanding Article of the Year – Ethics Pays



2008 Association of Local Government Auditors' Bronze Website Award



2005 Institute of Internal Auditors' Award to IAD for Recognition of Commitment to Professional Excellence, Quality, and Outreach

 ORANGE COUNTY BOARD OF SUPERVISORS'
Internal Audit Department

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**
Director Certified Compliance & Ethics Professional (CCEP)
Certified Information Technology Professional (CITP)
Certified Internal Auditor (CIA)
Certified Fraud Examiner (CFE)
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



OC Fraud Hotline (714) 834-3608



Transmittal Letter



Audit No. 2948-A October 27, 2010

TO: CAPS Steering Committee:
David Sundstrom, Auditor-Controller, Chair
Bob Franz, Chief Financial Officer, Vice-Chair
Satish Ajmani, Chief Information Officer
Carl Crown, Human Resources Director
Shaun Skelly, Chief Deputy Auditor-Controller

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

SUBJECT: **Public Report** - CAPS Steering Committee -
Audit of CAPS+ Financial System Oracle
Database Configuration

We have completed an Information Technology Audit of the Oracle database configuration for the CAPS+ financial system as of January 31, 2010. We performed this audit in accordance with our *FY 2009-10 Audit Plan and Risk Assessment* approved by the Audit Oversight Committee and the Board of Supervisors. Our final report is attached for your review.

Because of the sensitivity of the issues and risks of disclosing specific details, we have issued this public report (2948-A) containing general information and a confidential report (2948-B) containing the specific details. The confidential report distribution was limited to the CAPS Steering Committee and selected personnel within CEO/Information Technology and Auditor-Controller.

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). As a matter of policy, 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.

Letter from Dr. Peter Hughes, CPA



We have attached a **Follow-Up Audit Report Form**. Your department should complete this template as our audit recommendations are implemented. When we perform our first Follow-Up Audit approximately six months from the date of this report, we will need to obtain the completed document to facilitate our review.

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.

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 public report are listed on the **OC Internal Auditor's Public Report** on page 5.

Table of Contents



Information Technology Audit:
Public Report
CAPS Steering Committee
CAPS+ Financial System Oracle Database Configuration
Audit No. 2948-A

As of January 31, 2010

Transmittal Letter	i
OC Internal Auditor's Public Report	
OBJECTIVES	1
BACKGROUND	2
SCOPE	3
SCOPE EXCLUSIONS	3
RESULTS	3
Public Detailed Findings, Recommendations and Management Responses	
1. Finding No. 1– Database Auditing/Logging (Significant Issue)	6
2. Finding No. 2 – Need to Establish Personal Accounts for DBAs (Control Finding)	7
3. Finding No. 3 – Account Profile Password Settings (Control Finding)	7
4. Finding No. 4 – Oracle Password Security Function (Control Finding)	7
5. Finding No. 5 – Account Profile Resource Settings (Control Finding)	8
6. Finding No. 6 – Listener Configuration Settings (Control Finding)	8
7. Finding No. 7 – Additional Listener Functionality (Control Finding)	9
8. Finding No. 8 – Unnecessary User “Read” Access Granted to the Oracle Database (Control Finding)	9
9. Finding No. 9 – Changing User Account Passwords (Control Finding)	9
10. Finding No. 10 – Other Oracle Security Features Not Utilized (Control Finding)	10
ATTACHMENT A: Report Item Classifications	12
ATTACHMENT B: CAPS Steering Committee Responses	12



Audit No. 2948-A

October 27, 2010

TO: CAPS Steering Committee:
David Sundstrom, Auditor-Controller, Chair
Satish Ajmani, Chief Information Officer
Bob Franz, Chief Financial Officer, Vice-Chair
Carl Crown, Human Resources Director
Shaun Skelly, Chief Deputy Auditor-Controller

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

SUBJECT: **Public Report** - CAPS Steering Committee – Audit of
CAPS+ Financial System Oracle Database Configuration

Audit Highlight

We audited the CAPS+ Financial System Oracle Database Configuration as of January 31, 2010. The County of Orange implemented CAPS+ on July 1, 2009 as its enterprise financial system of record. The CAPS+ financial system uses Oracle 10g as its database management software. Although the CAPS+ financial system contains mainly non-confidential information, it does contain some sensitive or protected information.

We found that the Oracle database configuration was generally configured to secure the CAPS+ financial system data, but there are enhancements that can and should be made to provide better security. We identified one **(1) Significant Issue** and **nine (9) Control Findings** to improve configurations, controls, and processes for the Oracle database.

OBJECTIVES

The Internal Audit Department conducted an Information Technology Audit of the CAPS+ Financial System Oracle Database Configuration.

The objective of our audit was to determine whether the Oracle database was configured to secure the CAPS+ financial system data. We reviewed the Oracle database configuration (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 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.



- 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.

BACKGROUND

The County of Orange implemented CAPS+ on July 1, 2009, as its enterprise financial system to record general ledger, fixed asset, cost accounting, purchasing, cash receipting, and accounts payable transactions. The CAPS+ financial system uses Oracle 10g as its database management software. Although the CAPS+ financial system contains mainly non-confidential information, it does contain some sensitive or protected information.

The CAPS+ financial system is overseen by the CAPS Steering Committee. The CAPS Steering Committee establishes priorities, allocates resources, provides executive oversight and guidance, and makes policy and other critical decisions. As members of the CAPS Steering Committee, the personnel of the Auditor-Controller, CEO/Procurement, and CEO/Budget also direct and support decisions related to the functional or end user policies and processes.

The CAPS Steering Committee is supported by the CAPS Program Management Office (PMO) located within the Auditor-Controller. In addition to providing oversight and budgetary support for the CAPS+ financial system, the CAPS PMO is also responsible for supporting system users with Countywide training, documentation, help desk, communication, and outreach programs.

The CAPS+ financial system was developed by a third-party (CGI Technologies and Solutions Inc.), was customized to meet the County's requirements, and is licensed to the County. The application is supported as follows:

- CGI Platinum support provides application software enhancements which incorporate the County's customizations.
- CEO/Information Technology (CEO/IT) performs its duties for the CAPS+ financial system at the direction of the CAPS PMO. CEO/IT is responsible for maintaining the hardware, operating system, and database software (database creation, maintenance, backup and recovery, data refreshes, and implementing data security). In addition, they perform the software migration from non-production to production environment, database monitoring (to ensure proper functioning), job scheduling, and system backups. In general, CEO/IT supports the "physical layer" of the CAPS+ data model.
- Auditor-Controller Information Technology (A-C/IT) is responsible for supporting all other technical aspects of the CAPS+ financial system including ownership of the data (defining database configurations) and data security. In general, A-C/IT supports the "conceptual" and "logical" layers of the CAPS+ data model.

The CAPS+ production environment consists of servers providing the following functionality: Web, Application, Database (Finance and Data Warehouse), InfoAdvantage, ETL, and Forms Processing. The non-production environment includes: Application/Web, Database, and Forms Processing.



The CAPS+ financial system data may be accessed via:

- CAPS+ Application: access is authenticated directly by the application.
- Oracle Database: access is authenticated by the database.
- Server: access is authenticated by the operating system.

SCOPE

Our audit was to determine whether the Oracle database was configured to secure the CAPS+ financial system data as of January 31, 2010.

We reviewed the Oracle database configuration for the CAPS+ financial system in the following areas: Account Profiles, Privileges and Authorizations, Listener, Data Security, Operating System, Database Links, Auditing/Logging, Authentication, Database Parameters, and Other Related Oracle Database Security Features. See further description of these areas on page 1 above.

SCOPE EXCLUSIONS

Our audit did not include other aspects of the CAPS+ financial system including the following:

- Firewalls.
- Hardware controls including configuration. We did review operating system access controls (directory permissions) over the Oracle database files and data.
- Application controls including configuration (workflow), authentication, authorization (user roles), and logging/audit trails.
- Oracle database InfoAdvantage instance or any other instances except for the production CAPS+ financial system.

While our scope did not cover these non-production environments, the findings and recommendations would also be applicable to those environments.

These recommendations will be even more important when the new CAPS+ Human Resources/Payroll System is implemented on January 1, 2011.

RESULTS

We found that the Oracle database was generally configured to secure the CAPS+ financial system data, but there are enhancements that can and should be made to provide better security. We identified **one (1) Significant Issue** and **nine (9) Control Findings** resulting in **ten (10) recommendations** to improve configurations, controls, and processes as discussed in the *Detailed Findings, Recommendations and Management Responses* section of this report. See *Attachment A* for a description of Report Item Classifications.



Because of the sensitivity of the issues and risks of disclosing specific details, we have issued this public report (2948-A) containing general information only. A separate confidential report (2948-B) containing the specific details was distributed to the CAPS Steering Committee and selected personnel within CEO/Information Technology and Auditor-Controller.

Based upon our audit, we noted:

- ▶ **Objective #1 – Oracle Database Configuration:** *For the CAPS+ financial system, determine whether the Oracle database was configured to secure the data.*

- ▶ **Results:** We found that the Oracle database was generally configured to secure the CAPS+ financial system data, but there are enhancements that can and should be made to provide better security. We noted **one (1) Significant Issue** and **nine (9) Control Findings** in the areas of Account Security, Listener, Auditing/Logging, and Other Related Oracle Database Security Features. (See pages 6 - 11)

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 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 Information Technology Audit enhances and complements, but does not substitute for CEO/Information Technology's and Auditor-Controller/Information Technology'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 CEO/Information Technology's and Auditor-Controller/Information Technology's controls and processes related to the CAPS+ Oracle database configuration.



Acknowledgment

We appreciate the courtesy extended to us by CEO/Information Technology and Auditor-Controller/Information Technology. If we can be of further assistance, please contact me directly; or Eli Littner, Deputy Director at 834-5899; or Autumn McKinney, Senior Audit Manager at 834-6106.

Attachments

Public Report Distribution Pursuant to Audit Oversight Committee Procedure No. 1:

Members, Board of Supervisors
Members, Audit Oversight Committee
Thomas G. Mauk, County Executive Officer
Mahesh Patel, Assistant CIO, CEO/Information Technology
Joel Manfredo, Chief Technology Officer, CEO/Information Technology
Sreesha Rao, Director Business Information Services, CEO/Information Technology
Sanjukta Chakraborty, DBA, 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



Audit Objective #1 – Oracle Database Configuration

Our objective was to determine whether the Oracle database was configured to secure the CAPS+ financial system data.

County's Oracle Database Configuration Strengths

Our audit determined that the Oracle database was generally configured to secure the CAPS+ financial system data. Configuration, process, and control strengths noted during the audit include:

- ✓ Privileges & Authorizations: Database users (assigned to individuals) have read access only with the exception of database administrators and system accounts (not assigned to individuals) which have additional privileges necessary to perform their function.
- ✓ Operating Security: Update access to operating system files and directories was limited to system owner accounts.
- ✓ Database Links: None configured.
- ✓ Other Oracle Parameter Settings: Configured to meet best practices.

The following are areas where configurations, processes, and controls can be enhanced:

1. Finding No. 1 – Database Auditing/Logging (Significant Issue)

Internal Audit determined that the Oracle database was not configured to perform sufficient auditing/logging. It is a best practice to monitor database activity with auditing/logging. When determining an auditing/logging strategy, the risks, costs/benefits, and performance impacts should be considered.

Because of the risks of disclosing specific details, the details of this finding have been removed to ensure the security of the database. A separate confidential report (2948-B) containing the specific details was provided to CAPS Steering Committee for corrective action.

Recommendation No. 1

We recommend that the CAPS Steering Committee ensure an auditing/logging strategy is developed and implemented for the CAPS+ Oracle database. Any sensitive/confidential tables should be logged and their accesses reviewed for appropriateness.

CAPS Steering Committee Response:

Concur, CAPS Steering team agrees that the level of auditing/logging on the CAPS+ Production database should be enhanced.

Estimated completion dates: July 2011 depending on the requirements for storage and resources necessary to review and monitor these logs.



2. Finding No. 2 – Need to Establish Personal Accounts for DBAs (Control Finding)

Internal Audit noted that personal accounts for the Oracle database administrators were not created to reduce the exposure of additional powerful accounts. Instead, the database administrators used the system accounts to perform their duties. Although some activities should be performed using the system accounts to ensure proper security, other activities should be performed with personal accounts to ensure accountability. Security best practices dictate that all users have uniquely identifiable accounts to ensure accountability.

Recommendation No. 2

We recommend that CEO/IT establish personal accounts for the database administrators to use when performing their duties whenever possible.

CAPS Steering Committee Response:

Concur. CEO-IT will create named database user accounts with DBA privileges for the database administrators.

Estimated completion dates: November 2010 as part of standard revisions.

3. Finding No. 3 – Account Profile Password Settings (Control Finding)

Internal Audit reviewed the account password profile settings and noted that they did not meet best practices. Appropriate password settings reduce the risk of unauthorized access.

Because of the risks of disclosing specific details, the details of this finding have been removed to ensure the security of the database. A separate confidential report (2948-B) containing the specific details was provided to CEO/IT for corrective action.

Subsequent to the completion of our fieldwork, Internal Audit verified the account password profile settings were subsequently changed by CEO/IT to reflect best practices.

Recommendation No. 3

No recommendation is needed as sufficient corrective action was quickly taken by CEO/IT after our fieldwork was completed.

CAPS Steering Committee Response:

Concur.

4. Finding No. 4 – Oracle Password Security Function (Control Finding)

Internal Audit determined that an Oracle password security function was not being utilized by CEO/IT. Appropriate password settings reduce the risk of unauthorized access.

Because of the risks of disclosing specific details, the details of this finding have been removed to ensure the security of the database. A separate confidential report (2948-B) containing the specific details was provided to CEO/IT for corrective action.

Subsequent to the completion of our fieldwork, Internal Audit verified the Oracle password function was subsequently implemented by CEO/IT.



Recommendation No. 4

No recommendation is needed as sufficient corrective action was quickly taken by CEO/IT after our fieldwork was completed.

CAPS Steering Committee Response:

Concur.

5. Finding No. 5 – Account Profile Resource Settings (Control Finding)

Internal Audit reviewed the account resource management settings and noted that they did not meet best practices. By limiting system resources used by user sessions, the risk to production availability and denial of service attacks is reduced.

Because of the risks of disclosing specific details, the details of this finding have been removed to ensure the security of the database. A separate confidential report (2948-B) containing the specific details was provided to CEO/IT for corrective action.

Subsequent to the completion of our fieldwork, Internal Audit verified the account resource management capabilities were subsequently modified by CEO/IT to reflect best practices.

Recommendation No. 5

No recommendation is needed as sufficient corrective action was quickly taken by CEO/IT after our fieldwork was completed.

CAPS Steering Committee Response:

Concur.

6. Finding No. 6 – Listener Configuration Settings (Control Finding)

Internal Audit reviewed the listener parameter settings and noted settings were not configured to meet best practices. If not configured properly, the Listener functionality may be used inappropriately.

Because of the risks of disclosing specific details, the details of this finding have been removed to ensure the security of the database. A separate confidential report (2948-B) containing the specific details was provided to CEO/IT for corrective action.

Recommendation No. 6

We recommend that CEO/IT modify the Listener configuration settings to meet best practices.

CAPS Steering Committee Response:

Concur. The configuration files in the database server are already protected by operating system file permissions and general security restrictions related to server access. CEO-IT DBA will set the listener configuration, as suggested.

Estimated completion dates: January 2011 pending further discussion with CGI.



7. Finding No. 7 – Additional Listener Functionality (Control Finding)

Additional Listener functionality was not configured to meet best practices. If not configured properly, the Listener functionality may be used inappropriately.

Because of the risks of disclosing specific details, the details of this finding have been removed to ensure the security of the database. A separate confidential report (2948-B) containing the specific details was provided to CEO/IT for corrective action.

Recommendation No. 7

We recommend that CEO/IT configure the Listener to meet best practice.

CAPS Steering Committee Response:

Concur, CEO-IT working with the applications team (AC-IT) and the CAPS PMO office, will implement any changes deemed necessary to the use of “external process functionality”. AC-IT will be obtaining information from the vendor of specifications for this parameter and test the changes implemented by CEO-IT in the non-production environment prior to implementation into the production environment.

Estimated completion dates: January 2011 pending further discussion with CGI.

8. Finding No. 8 – Unnecessary User “Read” Access Granted to the Oracle Database (Control Finding)

Internal Audit reviewed the list of Oracle database users and noted several usernames for individuals no longer associated with the CAPS+ implementation project or whose job duties do not appear to warrant the access. IT staff should not have access to the production system except as needed to perform their job responsibilities. Although these accounts only have “read” access, they may be used for unauthorized actions triggering Senate Bill (SB) 1386 notifications (California Security Breach Notification Act). California law requires the entity to notify affected individuals that their financial data has been disclosed to unauthorized parties. The CAPS+ financial system contains individual’s names and their associated bank account data which is covered by SB 1386.

Recommendation No. 8

We recommend that CEO/IT remove the unnecessary “Read” access to the Oracle database.

CAPS Steering Committee Response:

Concur, the user “read” accounts in the database are created in response to specific application support requirements from the AC-IT team. CEO-IT has taken the initiative to streamline the user access authorization changes requested by AC-IT and the CAPS PMO.

Estimated completion dates: January 2011 as part of a CEO-IT project to standardize access.

9. Finding No. 9 – Changing User Account Passwords (Control Finding)

Internal Audit determined that CEO/IT needed to improve its procedures for changing user account passwords.



Because of the risks of disclosing specific details, the details of this finding have been removed to ensure the security of the database. A separate confidential report (2948-B) containing the specific details was provided to CEO/IT for corrective action.

Subsequent to the completion of our fieldwork, Internal Audit verified that CEO/IT subsequently implemented improved procedures for changing user account passwords.

Recommendation No. 9

No recommendation is needed as sufficient corrective action was taken quickly by CEO/IT after our fieldwork was completed.

CAPS Steering Committee Response:

Concur, not required.

10. Finding No. 10 – Other Oracle Security Features Not Utilized (Control Finding)

Internal Audit determined that the following additional Oracle security features were not being utilized by CEO/IT:

- Oracle Wallet Manager: Password wallets provide the capability to store account credentials (passwords) in a secure manner including the ability to connect to the Oracle database using the wallet, which limits the exposure of passwords.
- SSL Authentication: SSL Authentication provides the capability to encrypt Oracle transmissions preventing unauthorized interception.
- Virtual Private Database: Security framework that implements Fine-Grained Access Control for tables, views, and synonyms.
- Oracle Database Vault: Security feature providing the ability to manage security from outside of the database to place better controls on privileged users including limiting their access to CAPS+ application data.
- Sql92 Security: Initial parameter setting when set to "TRUE" enforces the requirement that a user must have "SELECT" privilege on a table in order to be able to execute "UPDATE" and "DELETE" statements using "WHERE" clauses on a given table. This prevents users from gaining information about tables they do not have access to such as the user table.

Although these security features are provided by Oracle and provide the above benefits, it is unknown whether they may cause processing problems for the CAPS+ financial system by creating access restrictions that conflict with the system's ability to access the database. Therefore, their use should be thoroughly researched before implementing.

CEO/IT should work with the A-C/IT, CAPS PMO, and CGI to research the above Oracle security features and implement those features that do not conflict with the CAPS+ financial system, adequately address risks, and are cost effective.



As the CAPS Steering Committee is the governing body for the CAPS+ financial system and there will be costs associated with implementing some of the above security features, CEO/IT should obtain approval from the CAPS Steering Committee.

Recommendation No. 10

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 to adequately address risks.

CAPS Steering Committee Response:

Concur, CEO-IT will be working with the applications team (AC-IT) and the CAPS PMO office to implement any new Oracle security features such as the Oracle database vault.

Estimated completion dates: July 2011 pending further investigation and budget impacts.



ATTACHMENT A: Report Item Classifications

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

Material Weaknesses:

Audit findings or a combination of Significant Issues that can result in financial liability and exposure to a department/agency and/or to the County as a whole. Management is expected to address "Material Weaknesses" brought to their attention immediately.

Significant Issues:

Audit findings or a combination of Control Findings that represent a significant deficiency in the design or operation of processes or internal controls. Significant Issues will generally require management's 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.



ATTACHMENT B: CAPS Steering Committee Responses



RECEIVED

OCT 20 2010

Memorandum

INTERNAL AUDIT
DEPARTMENT

October 26, 2010

TO: Peter Hughes, Director
Internal Audit Department

From: CAPS PMO Office *Steve Robinson*
CAPS Steering Committee (CSC)

SUBJECT: Response to Internal Audit Draft Report of Integrated Internal Control
Review Audit of CAPS+ Financial System Oracle Database Configuration

The following are our responses to the recommendation contained in the Audit of CAPS+ Financial System Oracle Database Configuration (Audit No. 2948-B).

Finding No. 1: There is no database auditing/logging performed (significant issue).

Recommendation: We recommend that the CAPS Steering Committee ensure an auditing/logging strategy is developed and implemented for the CAPS+ Oracle database. Any sensitive/confidential tables should be logged and their accesses reviewed for appropriateness.

CAPS Steering Committee Response: Concur, CAPS Steering team agrees that the level of auditing/logging on the CAPS+ Production database should be enhanced.

Estimated completion dates: July 2011 depending on the requirements for storage and resources necessary to review and monitor these logs.

Finding No. 2: Need to establish personal accounts for DBAs (control finding).

Recommendation: We recommend that CEO/IT establish personal accounts for the database administrators to use when performing their duties whenever possible.

CAPS Steering Committee Response: Concur. CEO-IT will create named database user accounts with DBA privileges for the database administrators.

Estimated completion dates: November 2010 as part of standard revisions



ATTACHMENT B: CAPS Steering Committee Responses (Continued)

Finding No. 3: Account Profile Password Settings Do Not Meet Best Practice (Control Finding).

Recommendation: No recommendation is needed as sufficient corrective action was quickly taken by CEO/IT after our fieldwork was completed.

CAPS Steering Committee Response: Concur

Finding No. 4: Password Verify Function Is Not Used (Control Finding).

Recommendation: No recommendation is needed as sufficient corrective action was quickly taken by CEO/IT after our fieldwork was completed.

CAPS Steering Committee Response: Concur

Finding No. 5: Account Profile Resource Settings Were Left as Default (Control Finding).

Recommendation: No recommendation is needed as sufficient corrective action was quickly taken by CEO/IT after our fieldwork was completed.

CAPS Steering Committee Response: Concur

Finding No. 6: Listener configuration settings do not meet best practices (control finding).

Recommendation: We recommend that CEO/IT modify the Listener configuration settings to meet best practices.

CAPS Steering Committee Response: Concur. The configuration files in the database server are already protected by operating system file permissions and general security restrictions related to server access. CEO-IT DBA will set the listener configuration, as suggested.

Estimated completion dates: January 2011 pending further discussion with CGI.

Finding No. 7: External processes functionality is allowed (control finding).



ATTACHMENT B: CAPS Steering Committee Responses (Continued)

Recommendation: We recommend that CEO/IT configure the Listener to meet best practice.

CAPS Steering Committee Response: Concur, CEO-IT working with the applications team (AC-IT) and the CAPS PMO office, will implement any changes deemed necessary to the use of "external process functionality". AC-IT will be obtaining information from the vendor of specifications for this parameter and test the changes implemented by CEO-IT in the non-production environment prior to implementation into the production environment.

Estimated completion dates: January 2011 pending further discussion with CGI.

Finding No. 8: Unnecessary user "Read" access granted to the Oracle database (control finding).

Recommendation: We recommend that CEO/IT remove the unnecessary "Read" access to the Oracle database.

CAPS Steering Committee Response: Concur, the user "read" accounts in the database are created in response to specific application support requirements from the AC-IT team. CEO-IT has taken the initiative to streamline the user access authorization changes requested by AC-IT and the CAPS PMO.

Estimated completion dates: January 2011 as part of a CEOIT project to standardize access.

Finding No. 9: More Secure Command Is Not Utilized When Changing User Account Passwords (control finding).

Recommendation: No recommendation is needed as sufficient corrective action was quickly taken by CEO/IT after our fieldwork was completed.

CAPS Steering Committee Response: Concur, not required.

Finding No. 10: Other Oracle security features not utilized (control finding).

Recommendation: We recommend that the CAPS Steering Committee ensure the above Oracle security features are researched and those features are implemented that



ATTACHMENT B: CAPS Steering Committee Responses (Continued)

do not conflict with the CAPS+ financial system and are cost effective to adequately address risks.

CAPS Steering Committee Response: Concur, CEO-IT will working with the applications team (AC-IT) and the CAPS PMO office to implement any new Oracle security features such as the Oracle database vault.

Estimated completion dates: July 2011 pending further investigation and budget impacts.

cc: David Sundstrom
Satish Ajmani
Carl Crown
Bob Franz
Shaun Skelly