

Internal Audit Department

O R A N G E C O U N T Y
5th Largest County in the USA

FINAL CLOSE-OUT

SECOND FOLLOW-UP AUDIT:

AUDITOR-CONTROLLER \$200M ACCOUNTS RECEIVABLE/ COLLECTION PROCESSES – IT RESULTS AS OF FEBRUARY 28, 2010

OVER \$200 MILLION
IN RECEIVABLES
PROCESSED ANNUALLY

The Auditor-Controller fully implemented or closed all recommendations noted in our original audit.

31 of our 37 audit recommendations were implemented or closed in our first follow-up audit and the 6 remaining were implemented in this second follow-up audit.

AUDIT No: 2849

ORIGINAL AUDIT No. 2428-B

REPORT DATE: MARCH 18, 2010

Director: Dr. Peter Hughes, MBA, CPA, CIA, 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



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



2008 Association of Local Government Auditors' Bronze Website Award



2005 Institute of Internal Auditors' Award 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

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. 2849 March 18, 2010

TO: David E. Sundstrom
Auditor-Controller

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

SUBJECT: **Second and Final Close-Out** Follow-Up
Audit of Integrated Internal Control Review
of Auditor-Controller Accounts Receivable
and Collection Processes – IT Results,
Original Audit No. 2428-B, Issued August
11, 2005

We have completed a Second Follow-Up Audit of Integrated Internal Control Review of Auditor-Controller Accounts Receivable and Collection Processes – IT Results. Our audit was limited to reviewing, as of February 28, 2010, actions taken to implement six (6) recommendations remaining from our First Follow-Up Audit report dated August 5, 2008 (Audit No. 2624). We conducted this Second Follow-Up Audit in accordance with the *FY 08-09 Audit Plan and Risk Assessment* approved by the Audit Oversight Committee and Board of Supervisors (BOS).

The results of our Second Follow-Up Audit are discussed in the **OC Internal Auditor's Report** following this transmittal letter. Because satisfactory corrective action has been taken for the six remaining audit recommendations, **this report represents the close-out of the original audit.**

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.

Attachment

Other recipients of this report are listed on the **OC Internal Auditor's Report** on page 3.

Table of Contents



*Second and Final Close-Out Follow-Up Audit of
Integrated Internal Control Review of Auditor-Controller
Accounts Receivable and Collection Processes – IT Results
(Original Audit No. 2428-B)
Audit No. 2849*

As of February 28, 2010

Transmittal Letter	i
OC Internal Auditor’s Report	1

OC Internal Auditor's Report



Audit No. 2849

March 18, 2010

TO: David E. Sundstrom
Auditor-Controller

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

SUBJECT: **Second and Final Close-Out** Follow-Up Audit: Integrated Internal Control Review of Auditor-Controller Accounts Receivable and Collection Processes – IT Results, Original Audit No. 2428-B, Issued August 11, 2005

Scope of Review

We have completed a Second Follow-Up Audit of the Integrated Internal Control Review of Auditor-Controller Accounts Receivable and Collection Processes – IT Results. Our audit was limited to reviewing, as of February 28, 2010, actions taken to implement the six (6) remaining recommendations from our First Follow-Up Audit report dated August 5, 2008 (Audit No. 2624).

The original audit contained thirty-seven (37) recommendations. Thirty-one (31) recommendations were implemented or closed and six (6) were in process of being implemented during our First Follow-Up Audit.

Background

The Auditor-Controller is the Chief Accounting Officer for the County and oversees its central accounting systems, including the Accounts Receivable and Collections Section.

On July 1, 2009, after our first follow-up audit, the Auditor-Controller transferred the Collection staff and duties to the Treasurer-Tax Collector. The Auditor-Controller continues to perform the Accounts Receivable duties and provide IT support of the Collection system (CUBS).

The scope of the original audit included a review of the application controls for the CUBS system and the general controls for the Auditor-Controller's local area network (LAN) on which CUBS resides.

CUBS: The Columbia Ultimate Business Systems' Revenue Plus Collector System (CUBS) serves as the subsidiary accounts receivable ledger. As such, the initial recording and subsequent collection of receivables are recorded in CUBS. Data in CUBS typically includes names, addresses, social security numbers, and occasionally electronic protected health information (ePHI) as described in the Health Insurance Portability and Accountability Act (HIPAA). CUBS is also used to generate collection notices, maintain collector activity, and produce aging and other management reports. CUBS resides on the Auditor-Controller's local area network (LAN) and is maintained by the Auditor-Controller's Information Technology Division (IT). The CUBS server is located at the Enterprise Data Center (EDC), and the Auditor-Controller and Treasurer-Tax Collector staff remotely accesses it.



Results

Our Second Follow-Up Audit indicated the Auditor-Controller fully implemented the six (6) remaining recommendations. **As such, this report represents the final close-out of the original audit.** The following is the implementation status of the six (6) outstanding recommendations:

1. Remote Access Policies (Control Finding)

Auditor-Controller create written policies for administering remote access including periodic password changes for the modem.

Implemented. Remote access is no longer made by modem and is now made by Safeword tokens. The Auditor-Controller developed a Workforce Member Usage Document addressing remote access and implemented procedures to document remote access granted. This included using Help Desk software to document requests and actions taken as well as maintaining an inventory of Safeword tokens issued and returned. Because of corrective actions taken, we consider this recommendation implemented.

2. Remote Access Documentation (Control Finding)

Auditor-Controller document authorization for any remote access granted to its local area network.

Implemented. Remote access is no longer made by modem and is now made by Safeword tokens. Auditor-Controller developed a Workforce Member Usage Document addressing remote access and implemented procedures to document remote access granted. This included using the Help Desk software to document requests and actions taken as well as retaining signed copies of Workforce member Usage Documents. Because of corrective actions taken, we consider this recommendation implemented.

3. System Logs (Control Finding)

Auditor-Controller reconfigure its network operating system audit policies to record key security event activity, such as system events, policy changes, account management, and account logons.

Implemented. Our review of documentation provided by Auditor-Controller determined that the network is logging account logons activity but is not capturing system events, policy changes, or account management. Since the primary focus of our audit is CUBS and the CUBS server is configured to log system events, policy changes, account management, and account logon activity per best practices, we will consider this recommendation implemented.

4. System Log Review (Control Finding)

Auditor-Controller establish written procedures for reviewing the network operating system's audit log, including IT Manager review of changes to policy settings and security event activity.

Implemented. Auditor-Controller implemented procedures whereby the IT Director and IT support staff meet weekly to discuss network issues including audit log activity. In addition, IT support staff performs periodic reviews of network logs to ensure logging is being captured and backed up. Because of corrective actions taken, we consider this recommendation implemented.



5. **Employee Status Change Procedures (Control Finding)**

Auditor-Controller develop written procedures for notifying the IT Division of employee status changes.

Implemented. Auditor-Controller implemented a help desk solution which includes administration of user access. In addition, Auditor-Controller modified the Employee Separation Checklist to include steps to notify IT of employee separations and Local Security Administrator to remove employee's IBM system access. Because of corrective actions taken, we consider this recommendation implemented.

6. **Access Review (Control Finding)**

Auditor-Controller require resource owners to periodically review who has access to their data to ensure they remain appropriate. This review should be documented.

Implemented. Auditor-Controller implemented a help desk solution which includes administration of user access. Additionally, IT generates monthly reports of email account statistics, including last logon date, and distributes to Auditor-Controller Division Managers. While intended to address email capacity problems, the reports may also help identify user accounts that should be terminated. Because of corrective actions taken, we consider this recommendation implemented.

We appreciate the cooperation and assistance extended to us by Auditor-Controller 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 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
Shaun M. Skelly, Senior Director, A-C Accounting & Technology
Phil Daigneau, Director, A-C Information Technology
Jan Grimes, Director, A-C Central Accounting Operations
Claire Moynihan, Senior Manager, A-C Financial Reporting & Analysis
Vivienne Thornton, Manager, A-C Accounts Receivable & Collections
Foreperson, Grand Jury
Darlene J. Bloom, Clerk of the Board of Supervisors