Internal Audit Department

OC Board of Supervisors'

ORANGE COUNTY

FIRST FOLLOW-UP AUDIT: INTEGRATED INTERNAL CONTROL REVIEW OF THE AUDITOR-CONTROLLER ACCOUNTS RECEIVABLE AND COLLECTION PROCESSES – IT RESULTS

As of May 30, 2008

The original audit report contained thirty-seven (37) recommendations. Our Follow-Up Audit indicated that the Auditor-Controller took satisfactory corrective action to fully implement sixteen (16) recommendations. We also closed out another fifteen (15) recommendations.

Our original audit covered the information technology controls supporting the accounts receivable and collection processes, in which the Auditor-Controller's Accounts Receivable and Collections Unit processed approximately $200 million in receivables annually.

AUDIT NO: 2624
REPORT DATE: AUGUST 5, 2008

Audit Director: Peter Hughes, Ph.D., MBA, CPA
Deputy Director: Eli Littner, CPA, CIA
Sr. Audit Manager: Autumn McKinney, CPA, CIA
Audit Manager: Lily Chin, CPA

ORANGE COUNTY OCgov.com
Our Community. Our Commitment.

Internal Audit Department

Serving the OC Board of Supervisors since 1995

2007 Association of Local Government Auditors' Bronze Website Award

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

Independence Objectivity Integrity

Internal Audit Department

Providing Facts and Perspectives Countywide

Dr. Peter Hughes	**Ph.D., MBA, CPA, CCEP, CITP, CIA, CFE**
Office of The 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 J. 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

Letter from Director Peter Hughes

Transmittal Letter

AUDIT NO. 2624 AUGUST 5, 2008

TO: David E. Sundstrom
Auditor-Controller

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

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

We have completed our First 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 May 30, 2008, actions taken to implement the thirty-seven (37) recommendations made in our original audit report dated August 11, 2005. The results of our Follow-Up Audit are discussed in the **Internal Auditor's Report** following this transmittal letter.

At the request of the Audit Oversight Committee (AOC), we are to bring to their attention any audit recommendations we find still not addressed, resolved, or implemented after our Second Follow-Up Audit. The AOC requests that such open issues appear on the agenda at their next scheduled meeting for their discussion.

Because there are recommendations pending implementation, we have attached a **Second Follow-Up Audit Report Form**. Your department should complete this template as our audit recommendations are implemented. When we perform our second 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 Board of Supervisors (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 recommendation.

Attachments

Other recipients of this report listed on the Internal Auditor's Report on page 5.

Table of Contents

First 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
Audit No. 2624

As of May 30, 2008

Transmittal Letter	**i**
INTERNAL AUDITOR'S REPORT	**1**
Scope of Review	**1**
Results	**1**
Acknowledgement	**5**
ATTACHMENT A: Report Item Classifications	**6**
ATTACHMENT B: Auditor-Controller Management Responses	**7**

INTERNAL AUDITOR'S REPORT

AUDIT NO. 2624 **AUGUST 5, 2008**

TO: David E. Sundstrom
Auditor-Controller

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

SUBJECT: First Follow-Up Audit of the 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 First Follow-Up Audit of the Integrated Internal Control Review of Auditor-Controller Accounts Receivable and Collection Processes – IT Results. The scope of the original audit included a review of the application controls for the Columbia Ultimate Business Systems' Revenue Plus Collector (CUBS) System and the general controls for the Auditor-Controller's local area network (LAN) on which CUBS resided. Our follow-up audit was limited to reviewing corrective actions taken, as of May 30, 2008, to implement recommendations made in our original audit report dated August 11, 2005.

Results

The original audit report contained thirty-seven (37) recommendations. Our First Follow-Up Audit found that of the 37 recommendations:

- Ten (10) recommendations are **fully implemented**.
- Six (6) recommendations are considered **fully implemented** as the CUBS server was relocated to the County's Data Center as discussed below in item 1.
- Four (4) recommendations related to business continuity plans are **closed** for follow-up purposes as discussed below in item 2.
- Eleven (11) recommendations related to less significant general controls (not specific to CUBS) are **closed** for follow-up purposes as discussed below in item 3.
- Six (6) recommendations are **not implemented** and require action as discussed below in item 4.

We believe the remaining six (6) recommendations are still appropriate and further efforts should be made to fully implement them. The recommendations that have not been fully implemented are noted below along with a comment on their status. The item number from the August 11, 2005 report is shown in parentheses after each heading.

1. Relocation of CUBS Server to County Data Center (Nos. 18, 19, 21, 22, 23, and 24) – **Fully Implemented**:

   The original audit included 6 recommendations related to physical access and environmental controls for the Auditor-Controller's local area network server room where the CUBS server was located. In November 2007, the Auditor-Controller moved the CUBS server to the County's Data Center which has better physical access and environmental controls. Therefore, we consider these 6 recommendations to be "**fully implemented**" for the CUBS server for follow-up purposes.

2. Business Continuity Planning (Nos. 14, 17, 26, and 27) - **Closed**:

   The original audit included 4 recommendations related to business continuity planning. The Auditor-Controller has made progress in this area by storing back-up tapes for the CUBS server off-site. As part of a Countywide initiative by CEO/Office of Information Technology, the Auditor-Controller has also been working on developing a comprehensive business continuity plan (BCP) that includes the CUBS system. The Auditor-Controller's BCP is not fully completed yet, such as testing of the BCP. As there is a Countywide initiative to ensure completion of the Auditor-Controller's BCP, we will not pursue these recommendations further and will consider them "**closed**" for follow-up purposes.

3. Less Critical General IT Controls (Nos. 4, 13, 20, 25, 29, 30, 31, 32, 33, 34, and 35) - **Closed**

   The original audit included 11 recommendations to improve general information technology controls and were not specific to the CUBS system. The Auditor-Controller did not implement these 11 recommendations. We consider these 11 recommendations to be less critical and do not warrant our further evaluation. Therefore, we will consider them to be "**closed**" for follow-up purposes.

4. Recommendations Requiring Action (Nos. 6, 7, 9, 10, 11, and 12) – **Not Implemented**:

   The below 6 recommendations were not implemented and continue to warrant the Auditor-Controller's implementation:

   - No. 6: We recommend that the Auditor-Controller create written policies for administering remote access including periodic password changes for the modem. (Note: Remote access is now acquired using Safeword tokens and not a modem).
   - No. 7: We recommend that the Auditor-Controller document authorization for any remote access granted to its local area network.
   - No. 9: We recommend that the 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.
   - No. 10: We recommend that the 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.
   - No. 11: We recommend that the Auditor-Controller develop written procedures for notifying the IT Division of Employee status changes.
   - No. 12: We recommend that the Auditor-Controller require resource owners to periodically review who has access to their data to ensure they remain appropriate. This review should be documented.

   Auditor-Controller's Planned Action:

   - No. 6: We concur and have created an updated draft Workforce Member Usage Document that will be reviewed and signed by all Auditor-Controller employees (Ref Userid and Password Section). Related to passwords, the remote access follows the same policy implemented by CEO/IT requiring passwords to be changed every 90 days. This draft document will be finalized by the end of December 2008.

   - No. 7: We concur and have documented this in the draft IT Security Policy, Section 7.2.4: Remote Access. This draft document will be finalized by the end of December 2008.

   - No. 9: We concur, but this requires programming to develop script which will monitor operating system logs. The process will email the Auditor-Controller IT Director documentation of critical changes in addition to creating a file of changes for weekly review.

This methodology will be developed and included in the IT security policy by the end of December 2008.

- No. 10: We concur in the development of the program methodology. As described in the previous response (No. 9), we will include weekly reviews of these reports at our Auditor-Controller IT desktop support meetings. This procedure will be developed and included in the IT security policy document. The implementation of this process will be completed by the end of December 2008.

- No. 11: We concur. A procedure will be developed with Auditor-Controller HR staff that will require that the IT division be formally notified of any employee changes. This procedure will be posted in the IT security policy. This procedure will be finalized by the end of December 2008.

- No. 12: We concur. The Auditor-Controller IT division will generate a listing of all active accounts residing on the Auditor-Controller domain. This list will be distributed to the division managers for review and confirmation twice a year. This procedure will be developed and posted in the IT security policy by the end of December 2008.

Acknowledgement

We appreciate the courtesy and cooperation extended to us by the personnel of Auditor-Controller's Information Technology Section and Accounts Receivable/Collections Section during our audit. If you have any questions regarding our audit, please call 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

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 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 do not present a material exposure throughout the County. They generally will require prompt corrective actions.

- **Control Findings and/or Efficiency/Effectiveness Issues:**
  Audit findings that require management's corrective action to implement or enhance processes and internal controls. Control Findings and Efficiency/Effectiveness issues are expected to be addressed within our follow-up process of six months, but no later than twelve months.

ATTACHMENT B: Auditor-Controller Management Responses

AUDITOR-CONTROLLER
COUNTY OF ORANGE

HALL OF FINANCE AND 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

SHAUN M. SKELLY
SENIOR DIRECTOR
ACCOUNTING & TECHNOLOGY

JAN E. GRIMES
DIRECTOR
CENTRAL ACCOUNTING OPERATIONS

WILLIAM A. CASTRO
DIRECTOR
SATELLITE ACCOUNTING OPERATIONS

PHILLIP T. BAIGNEAU
DIRECTOR
INFORMATION TECHNOLOGY

DAVID E. SUNDSTROM, CPA
AUDITOR-CONTROLLER

August 1, 2008

TO: Peter Hughes, Director
Internal Audit Department

SUBJECT: Updated Draft Report on First Follow-Up Audit on the Integrated Internal Control Review of the Auditor-Controller Accounts Receivable and Collection Processes – IT Results, Audit No. 2624

Following is our updated response to the recommendations contained in the Draft Report on the First Follow-Up Audit on the Integrated Internal Control Review of the Auditor-Controller Accounts Receivable and Collection Processes - IT Results.

Recommendation No. 6: We recommend that the Auditor-Controller create written policies for administering remote access including periodic password changes for the modem (Note: Remote access is now acquired using Safeword tokens and not a modem).

Auditor-Controller Response: We concur and have created an updated draft Workforce Member Usage Document that will be reviewed and signed by all Auditor-Controller employees (Ref Userid and Password Section). Related to passwords, the remote access follows the same policy implemented by CEO/IT requiring passwords to be changed every 90 days. This draft document will be finalized by the end of December 2008.

Recommendation No. 7: We recommend that the Auditor-Controller document authorization for any remote access granted to its local area network.

Auditor-Controller Response: We concur and have documented this in the draft IT Security Policy, Section 7.2.4: Remote Access. This draft document will be finalized by the end of December 2008.

Recommendation No. 9: We recommend that the 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.

Auditor-Controller Response: We concur, but this requires programming to develop script which will monitor operating system logs. The process will email the Auditor-Controller IT Director documentation of critical changes in addition to creating a file of changes for weekly review. This methodology will be developed and included in the IT security policy by the end of December 2008.

ATTACHMENT B: Auditor-Controller Management Responses (continued)

Recommendation No. 10: We recommend that the 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.

Auditor-Controller Response: We concur in the development of the program methodology. As described in the previous response (No. 9), we will include weekly reviews of these reports at our Auditor-Controller IT desktop support meeting. This procedure will be developed and included in the IT security policy document. The implementation of this process will be completed by the end of December 2008.

Recommendation No. 11: We recommend that the Auditor-Controller develop written procedures for notifying the IT Division of Employee status changes:

Auditor-Controller Response: We concur. A procedure will be developed with Auditor-Controller HR staff that will require that the IT division be formally notified of any employee changes. This procedure will be posted in the IT security policy. This procedure will be finalized by the end of December 2008.

Recommendation No. 12: We recommend that the Auditor-Controller require resource owners to periodically review who has access to their data to ensure they remain appropriate. This review should be documented.

Auditor-Controller Response: We concur. The Auditor-Controller IT division will generate a listing of all active accounts residing on the Auditor-Controller domain. This list will be distributed to the division managers for review and confirmation twice a year. This procedure will be developed and posted in the IT security policy by the end of December 2008.

David E. Sundstrom
Auditor-Controller

PD:lr (Resp—First Follow-up AR & Collections IT Results Updated/depac)

cc: Shaun 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 Manger, A-C Financial Reporting & Analysis
Vivienne Thornton, Manager, A-C Accounts Receivable & Collections
Maribel Garcia, OC Internal Audit Department