# FIRST FOLLOW-UP AUDIT

# INTERNAL CONTROL AUDIT: AUDITOR-CONTROLLER'S AND TREASURER-TAX COLLECTOR'S \$22 BILLION ELECTRONIC FUNDS TRANSFER PROCESSES

# ORIGINAL AUDIT No. 2821

AS OF MAY 15, 2011

Our First Follow-Up Audit found that the Auditor-Controller, Treasurer-Tax Collector, and CEO/Information Technology fully implemented or closed six (6) recommendations, seven (7) recommendations are in process, and two (2) recommendations are not implemented from our original audit report dated October 14, 2010. For the period of March 2008 through March 2009, the Auditor-Controller and Treasurer-Tax Collector processed over \$22 billion in EFT transactions.

> AUDIT NO: 1033-C REPORT DATE: JUNE 29, 2011

Director: Dr. Peter Hughes, Ph.D., CPA Deputy Director: Eli Littner, CPA, CIA Senior Audit Manager: Michael Goodwin, CPA, CIA Senior IT Audit Manager: Autumn McKinney, CPA, CIA, CISA IT Audit Manager: Wilson Crider, CPA, CISA Senior Internal Auditor: Lisette Free, CPA

#### **RISK BASED AUDITING**

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

AICPA 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

≻

Z

O

ш

0

∡

Ľ

0

77

### Corange county board of supervisors' Internal Audit Department

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

**Providing Facts and Perspectives Countywide** 

#### **RISK BASED AUDITING**

<i>Dr. Peter Hughes</i> Director	Ph.D., MBA, CPA, CCEP, CITP, CIA, CFE, CFF Certified Compliance & Ethics Professional (CCEP) Certified Information Technology Professional (CITP)
	Certified Internal Auditor (CIA) Certified Fraud Examiner (CFE)
E-mail:	Certified in Financial Forensics (CFF) peter.hughes@iad.ocgov.com
Eli Littner Deputy Director	CPA, CIA, CFE, CFS, CISA Certified Fraud Specialist (CFS) Certified Information Systems Auditor (CISA)
Michael Goodwin Senior Audit Manager	CPA, CIA
Alan Marcum Senior Audit Manager	MBA, CPA, CIA, CFE
Autumn McKinney Senior Audit Manager	CPA, CIA, CISA, CGFM 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: <u>www.ocgov.com/audit</u>



OC Fraud Hotline (714) 834-3608

## Letter from Dr. Peter Hughes, CPA



### **Transmittal Letter**

Audit No. 1033-C June 29, 2011

- TO: David Sundstrom, Auditor-Controller Shari L. Freidenrich, Treasurer-Tax Collector Mahesh Patel, Acting Deputy CEO/CIO
- **FROM:** Dr. Peter Hughes, CPA, Director Internal Audit Department
- **SUBJECT:** First Follow-Up Audit of Internal Control Audit: Auditor-Controller's and Treasurer-Tax Collector's \$22 Billion Electronic Funds Transfer Processes, Original Audit No. 2821, Issued October 14, 2010

We have completed a First Follow-Up Audit of internal controls over the Auditor-Controller's and Treasurer-Tax Collector's \$22 Billion Electronic Funds Transfer Processes. Our audit was limited to reviewing, as of May 15, 2011, actions taken to implement the **fifteen (15) 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 Auditor-Controller, Treasurer-Tax Collector, and CEO/Information Technology fully implemented or closed six (6) recommendations, seven (7) recommendations are in process, and two (2) recommendations have not been implemented.

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 7.

# **Table of Contents**

First Follow-Up Audit of Internal Control Audit: Auditor Controller's and Treasurer-Tax Collector's \$22 Billion Electronic Funds Transfer Processes Audit No. 1033-C

As of May 15, 2011

Transmittal Letter	i
OC Internal Auditor's Report	1

### Audit No. 1033-C

June 29, 2011

- TO: David Sundstrom, Auditor-Controller Shari L. Freidenrich, Treasurer-Tax Collector Mahesh Patel, Acting Deputy CEO/CIO
- FROM: Dr. Peter Hughes, CPA, Director Studying Hes
- SUBJECT: First Follow-Up Audit of Internal Control Audit: Auditor-Controller's and Treasurer-Tax Collector's \$22 Billion Electronic Funds Transfer Processes, Original Audit No. 2821, Issued October 14, 2010

#### Scope of Review

We have completed a First Follow-Up Audit of the Internal Control Audit of the Auditor-Controller's and Treasurer-Tax Collector's Electronic Funds Transfer Processes. Our audit was limited to reviewing actions taken as of May 15, 2011 to implement the **fifteen (15) recommendations** made in our original audit report.

#### Background

The original audit reviewed internal controls over the Auditor-Controller's and Treasurer-Tax Collector's Electronic Funds Transfer (EFT) Processes, which included an evaluation of internal controls for:

- Establishing, authorizing, and processing electronic funds transfers completely and accurately in the A-C and T-TC;
- Segregation of duties in the Quantum and Commercial Electronic Office systems, including application controls related to user access profiles, system enforced dual authorizations, and password settings; and
- Access and transmission of A-C and T-TC EFT payment files transmitted to Wells Fargo Bank.
- In addition, we reviewed the processes for efficiencies and effectiveness.

For the period of March 2008 through March 2009, the A-C and T-TC processed over **\$22 billion** in EFT transactions. The original audit identified fifteen (15) **Control Findings**.

#### Results

Our First Follow-Up Audit indicated the Auditor-Controller, Treasurer-Tax Collector and CEO/Information Technology fully implemented or closed six (6) recommendations, seven (7) recommendations are in process, and two (2) recommendations have not been implemented. We believe the remaining nine (9) recommendations are still appropriate and further efforts should be made to fully implement them.

Based on the Follow-Up Audit we conducted, the following is the implementation status of the fifteen (15) original recommendations.



### 1. <u>Approval Signatures Not on Authorized List</u> (Control Finding)

Auditor-Controller ensure its Satellite Accounting Units verify the payment approval with the corresponding agency's authorized signature forms/access request forms prior to processing EFT payments.

<u>Current Status:</u> In Process. Satellite Accounting Units were sent an email on June 23, 2010 reminding them to verify authorized signatures. Draft written procedures for *Access Request Forms (ARF) Authorized Signature Validation* have been prepared, but have not been finalized. We tested sixteen (16) EFT transactions and related *On Demand Wire Forms* to determine if payment approval signatures were on the corresponding ARF and no exceptions were noted. Because A-C Claims & Disbursing is in process of finalizing written policies and procedures for verifying authorized signatures, we consider this recommendation in process.

#### Planned Action:

The Auditor-Controller plans to finalize and distribute written policies and procedures for verifying payment approval signatures to Satellite Accounting Units by December 2011.

#### 2. Missing Authorized Signatures on EFT/On Demand Wire Forms (Control Finding)

Auditor-Controller Check Writing ensure that hard copy *EFT/On Demand Wire Forms* contain authorized signatures before releasing payments.

<u>Current Status:</u> In Process. The A-C Check Writing Unit was verbally reminded to review authorized signatures prior to submitting the documents in CAPS+. Draft written procedures for *On Demand Wires* have been prepared, but have not been finalized. Our testing of sixteen (16) EFT transactions and corresponding ARFs found no exceptions. Because A-C Claims & Disbursing is in process of finalizing written policies and procedures to ensure authorized signatures are documented, we consider this recommendation in process.

#### Planned Action:

The Auditor-Controller plans to finalize written policies and procedures for ensuring authorized signatures are documented by December 2011.

#### 3. Data Entry Errors Not Detected (Control Finding)

Auditor-Controller Claims & Disbursing ensure payment processors adequately review the data entered against supporting documentation, including vendor addresses, to ensure it is accurate and complete prior to processing payments.

<u>Current Status:</u> In Process. A-C Check Writing was verbally reminded to review the input of vendor names prior to submitting General Accounting Trust (GAT) payment documents. For miscellaneous and GAT payments that are work-flowed and submitted to A-C Check Writing, A-C Claims & Disbursing is in process of developing written policies and procedures to ensure payment processors review vendor names and addresses. Two (2) exceptions were noted in our testing of sixteen (16) EFT transactions. Because A-C Claims & Disbursing is in process of finalizing written policies and procedures to ensure payment processors review data against supporting documentation, we consider this recommendation in process.



#### Planned Action:

The Auditor-Controller plans to finalize written policies and procedures for reviewing miscellaneous and GAT payments by December 2011.

#### 4. Payment Authorization Procedures Not Standardized (Control Finding)

Auditor-Controller should evaluate if standardized policies and procedures for authorizing and approving disbursements can be established to ensure they are consistently applied both in A-C Claims & Disbursing and the A-C Satellite Accounting Units. The standardized procedures should include scope of the reviews and specific review criteria that can be incorporated into department/agency policy and procedures.

<u>Current Status:</u> In Process. Draft uniform policies and procedures for *Payment Voucher & On Demand Wire (ODW) – Over Limit and Miscellaneous Vendor Code Approvals* have been prepared, but not finalized or distributed to Satellite Accounting Units. Additionally, a revised ODW form has been drafted. Because A-C Claims & Disbursing is in process of finalizing uniform policies and procedures to ensure standardization of payment reviews and approvals in A-C Claims & Disbursing and A-C Satellite Accounting Units, we consider this recommendation in process.

#### Planned Action:

The Auditor-Controller plans to finalize and distribute written policies and procedures for payment reviews and approvals to Satellite Accounting Units by December 2011.

#### 5. <u>Payment Authorization Procedures Not Standardized</u> (Control Finding)

Auditor-Controller should also evaluate whether disbursements processed as department <u>interfaces</u> should be subject to Auditor-Controller review and approval thresholds described above, and if support documentation should be required as part of the review process.

<u>Current Status:</u> Not Implemented. The Auditor-Controller has not evaluated whether interface payments should be subject to review and approval thresholds and if supporting documentation should be required as part of the process. The Auditor-Controller's reduction in staffing is impacting completing this recommendation. Once staffing becomes available, the Auditor-Controller intends to evaluate interface payments. Because no action has yet been taken on this recommendation, we consider it not implemented.

#### Planned Action:

The Auditor-Controller's reduction in staffing is impacting completing this review. A risk assessment will be completed by December 2011.

#### 6. Errors and Omissions of Bank Account Numbers (Control Finding)

Auditor-Controller Claims & Disbursing Unit and Satellite Accounting offices ensure during their review that bank account codes and ABA numbers are correctly documented <u>prior</u> to approving EFTs.

<u>Current Status:</u> **Implemented.** In order to ensure accuracy of the bank account codes and ABA numbers, all ODW forms are now required to have attached the vendor/payee wiring instructions in order for A-C Claims & Disbursing to release the wire.

# **OC Internal Auditor's Report**



This new requirement was announced in the Auditor-Controller Claims and Disbursement Bulletin Issue 2011-01, dated April 15, 2011. Our testing of sixteen (16) EFT transactions found no exceptions concerning bank account codes and ABA numbers. Therefore, we consider this recommendation implemented.

7. <u>Remove CEO System EFT "Release" Role for EFT Manual Approvers</u> (Control Finding) Treasurer-Tax Collector should remove the "release" access within the CEO system for the two manual approvers of EFTs.

<u>Current Status:</u> **Implemented.** The Treasurer-Tax Collector has removed the "release" access for the two approvers. Therefore, we consider this recommendation implemented.

#### 8. More Restrictive Quantum Account and Password Settings (Control Finding)

Treasurer-Tax Collector should restrict user log-on, implementing password filters to provide more password complexity, and setting the password uniqueness to twelve passwords.

<u>Current Status:</u> **Implemented.** The Treasurer-Tax Collector changed the Quantum account and password settings to meet our recommendations, but did not restrict multiple user log-ons. After further research and testing, the Treasurer-Tax Collector determined that the multiple log-ons were needed to run the unattended batch scheduler jobs. They investigated purchasing additional software licenses to restrict the multiple log-ons, but found that it was not cost effective. We accept the Treasurer-Tax Collector's conclusion and consider this recommendation to be overall implemented.

#### 9. <u>Remove Unnecessary CAPS+ FTP Server Administrative Accounts</u>

(Control Finding) Auditor-Controller should remove any user accounts no longer needed to maintain the CAPS+ hardware/software.

<u>Current Status:</u> **In Process.** The Auditor-Controller is working with the OC Enterprise Data Center to remove users that no longer need access to the CAPS+ FTP servers and to develop a process to ensure the current user list is updated on a regular basis. Therefore, we consider this recommendation in process.

Planned Action:

The Auditor-Controller will ensure inactive accounts are de-provisioned by July 31, 2011. An eService request was submitted to the OC Enterprise Data Center on June 3, 2011. The Auditor-Controller will periodically evaluate the list of accounts for further de-provisioning.

10. <u>Remove Unnecessary OC Enterprise Data Center FTP Server Administrative</u> <u>Accounts</u> (Control Finding) CEO/IT should remove those administrative accounts for individuals no longer requiring access to the FTP server located at the OC Enterprise Data Center.



<u>Current Status:</u> **Implemented.** We reviewed user access to the OC Enterprise Data Center FTP server and determined the unnecessary accounts were deactivated. Therefore, we consider this recommendation implemented.

11. <u>Restrict OC Enterprise Data Center FTP Server Administrative Accounts</u> (Control Finding) CEO/IT should limit the FTP job accounts' log-on capabilities: 1) to the console by removing the RDP (remote access) capabilities and 2) restricting access to specific hours when the account is used to transfer its file.

<u>Current Status:</u> **Implemented.** We reviewed the administrative accounts and determined the following: accounts were limited to specific times in which they could log-on (for most accounts it's during business hours of 7 a.m. to 5 p.m.); the administrator account was removed from having remote access via RDP; the only group allowed remote access via RDP was the network administrators; and the remaining accounts are only able to log-on locally. Therefore, we consider this recommendation implemented.

**12.** <u>Disallow Generic FTP External Firewall Rule</u> (Control Finding) CEO/IT should remove the global/generic FTP rule for network traffic through the external firewall. At a minimum, the banking related FTP activity should be the priority.

<u>Current Status:</u> **Closed.** During the original audit, we recommended the removal of the FTP service because it was our understanding it was not necessary due to the CEO/IT file transfer software being used. Subsequent to the original audit, CEO/IT indicated that the FTP service is needed to support departments, vendors, and customers who are not using the CEO/IT file transfer software. To limit or restrict access to this FTP service, an authorized user ID and password must be approved and set-up prior to using the FTP service. Therefore, we consider this recommendation closed.

### 13. <u>Consider Consolidation of County FTP Activity (Control Finding)</u>

CEO/IT should work with the applicable departments/agencies to consider consolidating external FTP activity to the OC Enterprise Data Center FTP server.

<u>Current Status:</u> In Process. Prior to soliciting any consolidation of departmental external FTP activity, CEO/IT decided to upgrade its existing FTP solution. The OC Enterprise Data Center developed a proposal for an upgraded FTP solution that was approved by CEO/IT. As part of the upgrade, CEO/IT is working to implement a refreshed enterprise platform for both intra-County and external FTP secure transactions. We were informed that CEO/IT has completed their Enterprise Architecture review and has obtained the applicable software. As CEO/IT is making progress toward potential consolidation, we consider this recommendation in process.

#### Planned Action:

CEO/IT will continue implementing the new Enterprise Secure FTP solution to position the County to begin consolidating the file transfer activities in and out of the County. All current CEO/IT project milestones are on target. We have communicated this important enhanced service to the agencies and have held presentations with their staff, demonstrating the value and necessity of adoption.



Testing of base infrastructure has been completed. We are working with the agencies to ensure all who are willing and able to migrate to the new solution do so with the full support of CEO/IT resources and backing. A presentation to the agencies has been developed and a session was held in June 2011. We anticipate that CEO/IT controllable actions for this project will be implemented by January 2012. We rely heavily on agency willingness to adopt the solution and disengage from their existing systems, barring cost-prohibitive native dependencies limiting their ability to adopt.

#### 14. <u>Develop Standardized Policy for County FTP Activity</u> (Control Finding)

CEO/IT should also develop a single Countywide policy for administration of the FTP activity. The policy should consider including: standardized procedures/tools for administration of the FTP process; a requirement for CEO/IT (CISO) review of new FTP servers, maintenance of a centralized inventory of external FTP file transfers; maintenance of a single/centralized schedule for the FTP jobs; and identification of sensitive files.

<u>Current Status:</u> **In Process.** We were informed that CEO/IT has been working with the IT governance groups (OC-SWG, OC-TAG, and Technology Council) to develop a Countywide external FTP policy and procedure framework. The topic was first introduced at the January 2011 Domain Architecture Group meetings, but still requires revision before approval by the Technology Council. The draft policy framework deals with issues of data classification, encryption, audit logs, and external FTP administration and change management. As CEO/IT is making progress toward a Countywide FTP policy, we consider this recommendation in process.

#### Planned Action:

CEO/IT will continue working with the IT governance groups (OC-SWG, OC-TAG, Technology Council, and Sr. Executive Council) to develop a Countywide external FTP policy and procedure framework. The Governance Groups have been engaged about the audit findings and recommendations and begun work on a draft Policy. However, a few already-completed Policies (impacting ALL workforce members) are already in the new governance pipeline ahead of the draft FTP Policy. It is estimated the final policy will be approved by November, 2011.

#### 15. Importance of Quality Assurance Reviews (Control Finding)

Auditor-Controller Claims & Disbursing should continue performing annual Quality Assurance Reviews and enhance the review process to include lower dollar EFT payment requests and interface transactions to help detect any improper or non-compliant transactions.

<u>Current Status:</u> **Not Implemented.** The Auditor-Controller agrees with the importance of Quality Assurance Reviews. However, due to the reduction of A-C Claims & Disbursing staff, quality assurance reviews/compliance reviews are not being completed. The last compliance review performed by the A-C Compliance Unit covered FY 2007/08.

On March 2011, A-C Internal Audit and Staff Services completed a management advisory review of the compliance monitoring processes. This review resulted in fifteen (15) observations to A-C management with suggestions for improvement to the compliance monitoring process.



The report indicated that compliance monitoring had not been performed for the last two fiscal years, and there was no indication when compliance monitoring would resume due to staffing levels in the Compliance Unit. Because compliance reviews are not being completed, we consider this recommendation not implemented.

#### Planned Action:

The Auditor-Controller agrees with the importance of Quality Assurance Reviews. Due to the continued reduction of Central Claims staff, quality assurance reviews are not being completed. A risk assessment will be completed by December 2011.

We appreciate the assistance extended by the Auditor-Controller, Treasurer-Tax Collector, 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 Michael Goodwin, Senior Audit Manager at 834-6066, 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 Bob Franz, Deputy CEO, Chief Financial Officer Shaun Skelly, Chief Deputy Auditor-Controller Jan Grimes, Director, Central Accounting Operations, Auditor-Controller Victoria Ross, Senior Manager, Claims and Disbursing, Auditor-Controller Salvador Lopez, Claims Manager, Claims and Disbursing, Auditor-Controller Lisa Poma, Disbursing Manager, Claims & Disbursing, Auditor-Controller Phil Daigneau, Director, Information Technology, Auditor-Controller Paul Gorman, Chief Assistant Treasurer-Tax Collector Jennifer Burkhart, Assistant Treasurer-Tax Collector Kim Hansen, Cash Manager, Treasurer-Tax Collector Joel Manfredo, Chief Technology Officer, CEO/Information Technology KC Roestenberg, Director, CEO/IT - Enterprise IT Shared Services Mark Khanlar, Manager, CEO/IT Enterprise IT Shared Services/Network Platform Svcs. Foreperson, Grand Jury

Darlene J. Bloom, Clerk of the Board of Supervisors