

Internal Audit Department

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

FINAL CLOSE-OUT

SECOND FOLLOW-UP AUDIT

INFORMATION TECHNOLOGY AUDIT: TREASURER-TAX COLLECTOR'S CONTROLS OVER COMPLIANCE WITH PCI DSS

AS OF JANUARY 18, 2012

Our Second Follow-Up Audit found the Treasurer-Tax Collector and Auditor-Controller fully implemented the three (3) remaining recommendations from our original report.

Previously, the Treasurer-Tax Collector, Auditor-Controller, OC Public Works, CEO/Procurement, and OC Community Resources fully implemented nine (9) recommendations in our First Follow-Up Audit report dated July 14, 2011.

AUDIT NO: 1147-A
(Original Audit No. 2946)

REPORT DATE: FEBRUARY 28, 2012

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

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

GRC (Government, Risk & Compliance) Group 2010 Award to IAD as MVP in Risk Management



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

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)

Certified in Financial Forensics (CFF)

E-mail:

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: www.ocgov.com/audit



OC Fraud Hotline (714) 834-3608

Letter from Dr. Peter Hughes, CPA



Transmittal Letter



Audit No. 1147-A February 28, 2012

TO: Shari L. Freidenrich
Treasurer-Tax Collector

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

SUBJECT: **Second and Final Close-Out** Follow-Up
Audit of Information Technology Audit:
Treasurer-Tax Collector's Controls over
Compliance with PCI DSS, Original Audit
No. 2946, Issued October 21, 2010

We have completed a Second Follow-Up Audit of the Treasurer-Tax Collector's Controls over Compliance with Payment Card Industry Data Security Standard (PCI DSS). Our audit was limited to reviewing, as of January 18, 2012, actions taken to implement the **three (3) recommendations** remaining from our original audit. We conducted this Second Follow-Up Audit in accordance with the *FY 11-12 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. Our Second Follow-Up Audit found the Treasurer-Tax Collector and the Auditor-Controller **fully implemented** the **three (3)** remaining recommendations from the original audit.

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 5.

Table of Contents



***Second and Final Close-Out Follow-Up Audit of
Information Technology Audit:
Treasurer-Tax Collector's Controls over Compliance with PCI DSS
Audit No. 1147-A***

As of January 18, 2012

Transmittal Letter	i
OC Internal Auditor's Report	1
Scope of Review	1
Background	1
Results	2

OC Internal Auditor's Report



Audit No. 1147-A

February 28, 2012

TO: Shari L. Freidenrich, Treasurer-Tax Collector

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

SUBJECT: **Second and Final Close-Out** Follow-Up Audit of Information Technology Audit: Treasurer-Tax Collector's Controls over Compliance with PCI DSS, Original Audit No. 2946, Issued October 21, 2010

Scope of Review

We have completed a Second Follow-Up Audit of the Treasurer-Tax Collector's Controls over Compliance with Payment Card Industry Data Security Standard (PCI DSS). Our audit was limited to reviewing actions taken as of January 18, 2012 to implement the **three (3) recommendations** remaining from our First Follow-Up audit report dated July 14, 2011 (Audit No. 1050-A).

Background

The original audit reviewed the Treasurer-Tax Collector's controls over compliance with payment card industry data security standard. The primary objective of our audit was to:

1. **Determine Whether Treasurer-Tax Collector's Countywide Governance Policies and Procedures (Controls) Ensure Compliance with PCI DSS Validation Requirements:** Review the Treasurer-Tax Collector's Countywide governance policies and procedures regarding payment card processing to determine whether they are adequate to ensure compliance with PCI DSS Validation Requirements.

The secondary audit objectives were to perform the following for a sample of **five (5)** County departments including the Treasurer-Tax Collector:

2. **Determine Whether PCI DSS Validation Documentation Requirements Were Met:** Determine the County's merchant level for each payment card brand accepted by the sample departments. Then based on the merchant level, determine whether the sample departments submitted the appropriate PCI DSS validation documentation to the acquiring banks.
3. **Review County's Third Party Payment Card Processors and Equipment for Compliance:** Determine whether third party payment card processors and equipment used by the sample departments were certified PCI DSS compliant.
4. **Review Third Party Agreements for PCI DSS Compliance:** For the sample departments, review a sample of the third party agreements for payment card processors, operating management agreements, and cashiering systems/applications to determine whether they address PCI DSS compliance.

The original audit identified one (1) **significant issue** and eleven (11) **control findings**.

OC Internal Auditor's Report



Results

Our Second Follow-Up Audit indicated the Treasurer-Tax Collector and the Auditor-Controller **fully implemented the remaining three (3) recommendations**. Based on the two Follow-Up audits we conducted, the following is the implementation status of the twelve (12) original recommendations:

1. No Countywide Governance Policy and Procedure Regarding PCI DSS and the Validation Requirements (Significant Issue)

Recommendation was not required as corrective action has been taken by the Treasurer-Tax Collector to implement a Countywide policy.

Current Status: **Fully Implemented** at time of original report issuance (**First Follow-Up Audit**). Therefore, we consider this recommendation fully implemented.

2. No Countywide Governance Policy and Procedure Regarding Establishing Bank Accounts (Control Finding)

We recommend that the Treasurer-Tax Collector develop and distribute a Countywide governance policy for the establishment of bank accounts.

Current Status: **Fully Implemented (Second Follow-Up Audit)**. The Treasurer-Tax Collector developed and distributed a Countywide policy for the establishment and closure of bank accounts. The policy was completed on October 3, 2011, emailed and distributed at the County's November 2011 Department Head meeting. Therefore, we consider this recommendation to be implemented.

3. No Countywide Governance Policy and Procedure Regarding Establishing Merchant Accounts (Control Finding)

We recommend that the Treasurer-Tax Collector develop and distribute a Countywide governance policy for the establishment of merchant accounts.

Current Status: **Fully Implemented (Second Follow-Up Audit)**. The Treasurer-Tax Collector developed a Countywide policy for the establishment and closure of merchant accounts. The policy was completed on October 3, 2011, emailed and distributed at the County's November 2011 Department Head meeting. Therefore, we consider this recommendation to be implemented.

4. No Auditor-Controller Policy Regarding Payment Cards/Electronic Payments (Control Finding)

We recommend that the Auditor-Controller revise Accounting Manual No. C-4 - *Deposits* to address acceptance of payment cards.

Current Status: **Fully Implemented (Second Follow-Up Audit)**. The Auditor-Controller issued an updated "interim" policy on January 11, 2012 to address acceptance of payment cards. The Auditor-Controller informed us the policy was "interim" as another update will be made for additional items such as the new CAPS+ system processes. During the update, the Auditor-Controller should consider adding reconciliation and training policies related to payment cards.

OC Internal Auditor's Report



Additionally, the Treasurer-Tax Collector issued an updated countywide PCI DSS Policy on February 2, 2012. Based on the combined Auditor-Controller and Treasurer-Tax Collector policy updates, we consider this recommendation to be fully implemented.

5. **Treasurer-Tax Collector Forms Do Not Address PCI DSS** (Control Finding)

We recommend that the Treasurer-Tax Collector update the Agency Worksheet and Cash Management Checklist for Setting up New Merchant Accounts to address PCI DSS validation requirements.

Current Status: **Fully Implemented (First Follow-Up Audit).** The Treasurer-Tax Collector updated the Agency Worksheet and Cash Management Checklist for Setting Up New Merchant Accounts on April 19, 2011 to address PCI DSS validation requirements including referencing the County PCI DSS policy. Therefore, we consider this recommendation fully implemented.

6. **Increasing PCI DSS Awareness** (Control Finding)

Recommendation not required as corrective action has been taken by the Treasurer-Tax Collector to increase awareness of PCI DSS.

Current Status: **Fully Implemented** at time of original report issuance (**First Follow-Up Audit**). Therefore, we consider this recommendation fully implemented.

7. **Departments Did Not Complete/Submit Self-Assessment Questionnaires to Acquiring Banks** (Control Finding)

We recommend that the Treasurer-Tax Collector annually monitor and verify that each County department accepting payment cards completes and submits the applicable PCI DSS Self Assessment Questionnaire to the acquiring banks.

Current Status: **Fully Implemented (First Follow-Up Audit).** We reviewed the Treasurer-Tax Collector's monitoring of submissions for the 2010 filing period and noted that all departments submitted their Self Assessment Questionnaire (SAQ) and Attestation of Compliance to the merchant banks as required.

The Treasurer-Tax Collector also updated its Countywide Payment Card Industry Data Security Standards Policy (February 2011) requiring all departments to submit their SAQ and Attestation of Compliance to the Treasurer-Tax Collector for tracking compliance, regardless of the merchant bank, and clarifying that non-Wells Fargo merchants/departments are responsible for submitting their appropriate banks.

Based on the above, we consider this recommendation fully implemented.



8. Quarterly Network Security Scan for Treasurer-Tax Collector (Control Finding)

We recommend that the Treasurer-Tax Collector determine whether they are considered a level "3" merchant by Wells Fargo and whether they need to begin having quarterly network security scans performed by an Approved Scanning Vendor.

Current Status: **Fully Implemented (First Follow-Up Audit).** On August 13, 2010, the Treasurer-Tax Collector received confirmation from the Wells Fargo Bank Merchant Service Relationship Manager that a quarterly network security scan is not required. Therefore, we consider this recommendation fully implemented.

9. T-TC's Cashiering System Terminals/Payment Card Readers Are Not PCI DSS Compliant (Control Finding)

We recommend that the Treasurer-Tax Collector complete its project to replace the current cashiering system and payment card readers/terminals as soon as possible to limit the County's exposure.

Current Status: **Fully Implemented (First Follow-Up Audit).** We confirmed the Treasurer-Tax Collector's newly implemented cashiering system (J-Point) is Payment Application-Data Security Standard (PA-DSS) certified by reviewing the listing of compliant software maintained by the PCI Security Standards Council. Therefore, we consider this recommendation fully implemented.

10. County Third Party Agreements Do Not Address PCI DSS Requirements (Control Finding)

We recommend that the County Procurement Office work with County Counsel to develop standard terms and conditions to address PCI DSS and PA-DSS compliance for contracts with third party payment processors or for the purchase/lease of payment card equipment and systems/applications.

Current Status: **Fully Implemented (First Follow-Up Audit).** The CEO/Procurement Office and County Counsel completed the new bid/contract language titled PCI DSS Compliance during November 2010. The new County Term/Condition (#122) has been distributed to all County departments and is now available on the County Purchasing Intranet Website. Therefore, we consider this recommendation fully implemented.

11. County Third Party Agreements Do Not Address PCI DSS Requirements (Control Finding)

We recommend that the OCPW/Corporate Real Estate work with County Counsel to develop standard terms and conditions to address PCI DSS and PA-DSS compliance in the operating/property management agreements.

OC Internal Auditor's Report



Current Status: **Fully Implemented (First Follow-Up Audit).** OCPW/Corporate Real Estate worked with County Counsel and developed standard terms and conditions that address PCI DSS and PA-DSS compliance in the lease/real property agreements. The new terms and conditions are available on the County Intranet (Real Estate Portal). We reviewed the new standard terms and conditions which address PCI DSS and PA-DSS compliance. Therefore, we consider this recommendation fully implemented.

12. Third Party Processing Not Clear to User (Control Finding)

We recommend that the Treasurer-Tax Collector, OC Public Works, and OC Community Resources modify their payment acceptance web sites to clearly state that they are being directed to a third party for payment processing.

Current Status: **Fully Implemented (First Follow-Up Audit).** OC Community Resources modified their payment website at the time of the original audit report. We verified that the Treasurer-Tax Collector and OC Public Works modified their web payment page to display a notification to the customer that payment processing will be performed by a third party vendor payment processing website. Therefore, we consider this recommendation fully implemented.

We appreciate the assistance extended by the Treasurer-Tax Collector and Auditor-Controller during our Second Follow-Up Audit. If you have any questions, please contact me directly or Eli Littner, Deputy Director at 834-5899, or Autumn McKinney, Senior IT Audit Manager at 834-6106.

Distribution Pursuant to Audit Oversight Committee Procedure No. 1:

Members, Board of Supervisors
Members, Audit Oversight Committee
Paul Gorman, Chief Assistant Treasurer-Tax Collector
Rosanne De Vera, Assistant Cash Manager, Treasurer-Tax Collector
Shaun Skelly, Chief Deputy Auditor-Controller
Jan Grimes, Director, Auditor-Controller/Central Accounting Operations
Nancy Ishida, Manager, Auditor-Controller/Internal Audit and Staff Services
Susan Novak, Clerk of the Board of Supervisors
Foreperson, Grand Jury