



INTERNAL AUDIT DEPARTMENT
COUNTY OF ORANGE

Recipient of the Institute of Internal Auditors
Award for Excellence

Integrity ♦ Objectivity ♦ Independence

Management Letter
on
Audit of the Statement of Assets
Held by the County Treasury

At
December 31, 2005

AUDIT NUMBER: 2511

REPORT DATE: September 25, 2006

Audit Director:	Peter Hughes, Ph.D., CPA
Deputy Director:	Eli Littner, CPA, CIA, CISA
Audit Manager:	Alan Marcum, MBA, CPA, CIA
In-Charge Auditor:	Camille Gackstetter, CPA
Principal IT Auditor:	Scott Suzuki, CPA, CISA, CIA
Principal Auditor:	Nancy Ishida, CPA, CISA, CIA,
Senior Auditor:	Kenneth Wong, CPA, CIA

**MANAGEMENT LETTER ON AUDIT OF
STATEMENT OF ASSETS HELD BY COUNTY TREASURER
AT DECEMBER 31, 2005**

TABLE OF CONTENTS

Transmittal Letter.....	i
MANAGEMENT LETTER.....	1
EXECUTIVE SUMMARY	3
OBJECTIVES	3
BACKGROUND	3
CONCLUSION.....	3
DETAILED OBSERVATIONS, RECOMMENDATIONS AND MANAGEMENT RESPONSES	4
Segregation of Duties.....	4
Internal Controls Over Granting Network Access.....	5
IT Logical Security Controls	5
IT Security Monitoring Controls	6
IT Physical Security	7
Investment Policy Statement	8
ATTACHMENT A: Report Item Classifications	9
ATTACHMENT B: Treasurer-Tax Collector Management Responses.....	10



COUNTY OF ORANGE
INTERNAL AUDIT DEPARTMENT
Recipient of the Institute of Internal Auditors
Award for Excellence

Integrity ♦ Objectivity ♦ Independence

ELI LITTNER
CPA, CIA, CFE, CFS, CISA
DEPUTY DIRECTOR

MICHAEL J. GOODWIN
CPA, CIA
AUDIT MANAGER

ALAN MARCUM
MBA, CPA, CIA, CFE
AUDIT MANAGER

AUTUMN MCKINNEY
CPA, CIA, CGFM
AUDIT MANAGER

Office of the Director
DR. PETER HUGHES
Ph.D., MBA, CPA, CIA, CFE, CITP

MAILING ADDRESS:
400 CIVIC CENTER DRIVE WEST
BUILDING 12, ROOM 232
SANTA ANA, CALIFORNIA 92701

TELEPHONE: (714) 834-5475
FAX: (714) 834-2880

EMAIL: peter.hughes@ocgov.com
WEBSITE: www.ocgov.com/audit/

Transmittal Letter

Audit No. 2511

September 25, 2006

TO: John M. W. Moorlach, Treasurer-Tax Collector

FROM: Peter Hughes, Ph.D., CPA, Director
Internal Audit Department

SUBJECT: Management Letter on Audit of the Statement of Assets Held by the County Treasury at December 31, 2005

Attached is our Management Letter for the Audit of the Statement of Assets Held by the County Treasury at December 31, 2005. The Management Letter contains eleven audit recommendations, which includes **one Significant Issue**. Your responses to our recommendations have been included in the Management Letter and the complete text of the responses is included in Attachment B.

Please note, we implemented a more 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 now begin no later than six months upon the official release of the report. 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 now begin at 12 months from the release of the original 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.

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

As the Director of Internal Audit, I submit a monthly 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 department so 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 be forwarding to your department a Customer Survey of Audit Services for completion. Your department will receive the survey shortly after the distribution of this report.

Attachments

Other recipients of this report:

- Members, Board of Supervisors
- Members, Audit Oversight Committee
- Thomas G. Mauk, County Executive Officer
- David E. Sundstrom, Auditor-Controller
- Jan E. Grimes, Assistant Auditor-Controller, Central Operations
- Chriss W. Street, Assistant Treasurer-Tax Collector
- Paul C. Gorman, Deputy Treasurer
- Clarissa Adriano-Ceres, Deputy Treasurer-Tax Collector, Information Technology
- Foreperson, Grand Jury
- Darlene J. Bloom, Clerk of the Board of Supervisors



COUNTY OF ORANGE
INTERNAL AUDIT DEPARTMENT
Recipient of the Institute of Internal Auditors
Award for Excellence

Integrity ♦ Objectivity ♦ Independence

Office of the Director
DR. PETER HUGHES
Ph.D., MBA, CPA, CIA, CFE, CITP

MAILING ADDRESS:
400 CIVIC CENTER DRIVE WEST
BUILDING 12, ROOM 232
SANTA ANA, CALIFORNIA 92701

TELEPHONE: (714) 834-5475
FAX: (714) 834-2880

EMAIL: peter.hughes@ocgov.com
WEBSITE: www.ocgov.com/audit/

ELI LITNER
CPA, CIA, CFE, CFS, CISA
DEPUTY DIRECTOR

MICHAEL J. GOODWIN
CPA, CIA
AUDIT MANAGER

ALAN MARCUM
MBA, CPA, CIA, CFE
AUDIT MANAGER

AUTUMN MCKINNEY
CPA, CIA, CGFM
AUDIT MANAGER

MANAGEMENT LETTER

Audit No. 2511

September 25, 2006

TO: John M. W. Moorlach, Treasurer-Tax Collector

SUBJECT: Management Letter on Audit of the Statement of Assets Held by the County Treasury at December 31, 2005

Pursuant to Government Code §26920(b) and §26922, we have audited the Statement of Assets Held by the County Treasury as of December 31, 2005 and have issued our report dated April 28, 2006.

In planning and performing our audit, we considered the Treasury's internal controls in order to determine our auditing procedures for the purpose of expressing an opinion on the financial statement and not to provide overall assurance on the internal controls in place. However, we noted certain matters involving the internal controls and its operations that we consider being reportable conditions under the standards established by the American Institute of Certified Public Accountants. Reportable conditions involve matters coming to our attention relating to deficiencies in the design or operation of the internal control that in our judgment, could adversely affect the organization's ability to record, process, summarize, and report financial data consistent with the assertions of management in the financial statement. For purposes of reporting our audit observations and recommendations, we have classified audit report items into three distinct categories: Material Weaknesses, Significant Issues, and Control Findings. See Attachment A for a description of report item classifications.


We identified eleven audit findings, which includes **one Significant Issue**. No Material Issues were noted. These deficiencies are discussed in the Detailed Findings, Recommendations, and Management Responses section of this report and should be corrected to strengthen the internal controls and enhance assurance that internal control procedures are adequate to achieve reliability of financial reporting.

The Treasurer is responsible for establishing and maintaining the internal controls framework for his Department. In fulfilling this responsibility, judgments by management are required to assess the expected benefits and related costs of internal control policies and procedures.

The objectives of internal controls over financial reporting are to provide management with reasonable, but not absolute, assurance that reliability of financial reporting is achieved with established criteria and management's policies.

This report was discussed with representatives of the Treasury management; their responses have been incorporated in the report. This report is intended solely for the use of the Treasury management and should not be used for any other purpose. However, this report is a matter of public record and its distribution is not limited.

We appreciate the courtesy and cooperation extended to us by the personnel of the Treasury during our review. If we can be of further assistance, please contact me or Eli Littner, Deputy Director, at (714) 834-5899, or Alan Marcum, Audit Manager, at (714) 834-4119.



Peter Hughes, Ph.D., CPA
Director, Internal Audit

Audit Team:

Eli Littner, Deputy Director, CPA, CIA, CISA
Alan Marcum, Audit Manager, CPA, CIA
Camille Gackstetter, In-charge Auditor, CPA
Scott Suzuki, Principal IT Auditor, CPA, CISA, CIA
Nancy Ishida, Principal Auditor, CPA, CISA, CIA
Kenneth Wong, Senior Auditor, CPA, CIA

Attachment A – Report Item Classifications

Attachment B – Treasurer-Tax Collector Management Responses

Distribution Pursuant to Audit Oversight Committee Procedure No. 1:

Members, Board of Supervisors
Members, Audit Oversight Committee
Thomas G. Mauk, County Executive Officer
David E. Sundstrom, Auditor-Controller
Jan E. Grimes, Assistant Auditor-Controller, Central Operations
Chriss W. Street, Assistant Treasurer-Tax Collector
Paul C. Gorman, Deputy Treasurer
Clarissa Adriano-Ceres, Deputy Treasurer-Tax Collector, Information Technology
Foreperson, Grand Jury
Darlene J. Bloom, Clerk of the Board of Supervisors

EXECUTIVE SUMMARY

OBJECTIVES

The Internal Audit Department audited the Statement of Assets Held by the County Treasury as of December 31, 2005 and issued the audit report dated April 28, 2006. In planning and performing our audit, we considered the Treasury's internal controls in order to determine our auditing procedures for the purpose of expressing an opinion on the financial statements and not to provide overall assurance on the internal controls in place.

BACKGROUND

The audit was conducted for the purpose of assisting the Auditor-Controller in verifying the amount and kind of money and the amount of bank receipts in the treasury as shown on the Statement of Assets Held by the County Treasury as of December 31, 2005 (Statement), in accordance with Government Code §26920(b) and §26922.

CONCLUSION

Based on our audit of the Treasurer's Statement of Assets, we identified **one significant issue** and ten control findings which are noted in the Detailed Observations, Recommendations and Management Responses section of this report. No material weaknesses were noted. See Attachment A for a description of report item classifications.

The significant issue is related to one individual's combination of user permissions to execute Automated Clearing House (ACH) transactions. The ten control findings are related to the following: segregation of duties; network access; IT logical security controls over the Cashiering System; IT security monitoring (system changes and audit trails); IT physical security (back-up procedures, environmental controls, incident response plan, and disaster recovery plan testing); and revision to the Investment Policy Statement.



DETAILED OBSERVATIONS, RECOMMENDATIONS AND MANAGEMENT RESPONSES

The American Institute of Certified Public Accountants Statement on Auditing Standards, Section AU 319 – Consideration of Internal Control in a Financial Statement Audit requires auditors to obtain an understanding of the entity’s internal controls over relevant processes, as well as, consider the entity’s use of their information technology (IT) and its relevance to the audit of the financial statements. During the audit period, the Treasurer’s Office relied on information systems as their general ledger (Quantum System) and to record their cash (Cashiering and Back Office Systems), demand accounts and investments (Quantum System). Since the Treasurer’s Office relied on these information systems to provide the information on the financial statement, we gained an understanding of general and application controls of the systems, tested selected controls and identified the following weaknesses.

Segregation of Duties

Segregation of duties is a basic control that prevents or detects errors and irregularities by assigning responsibility for initiating transactions, recording transactions and custody of assets to separate individuals.

Finding No. 1: The Treasurer utilizes the Wells Fargo Bank Commercial Electronic Office application to send payroll taxes to governing agencies through Automated Clearing House (ACH) transactions. Transaction data is input by one employee, reviewed manually by a second employee, processed/released by the assistant cash manager, and subsequently reconciled by another employee. During our review of roles and responsibilities for the process, it was noted that one employee has inappropriate combination of user permissions to both edit and release an ACH transaction batch. These incompatible user permissions increase the risk of accidental or unauthorized changes to transactions that could result in the release of fraudulent ACH transactions. (Significant Issue)

Recommendation No. 1: We recommend the Treasurer revoke the employee’s permissions to both edit and release transaction batches.

Treasurer-Tax Collector Response: Concur – The Treasurer-Tax Collector’s (TTC) policy is to segregate the duties and the related Wells Fargo Bank Commercial Electronic Office user permissions to edit (or create) and release ACH transactions. The inappropriate combination of permissions occurred when making changes to reassign permissions and duties due to employee terminations. Once notified of the error, steps were taken immediately to make the necessary corrections. In addition, on April 3, 2006, we enabled a new security feature recently implemented by Wells Fargo Bank that prohibits users from creating and releasing the same ACH transactions regardless of individual user permissions.

Finding No. 2: Two individuals with cashiering and supervisory user access serve as cashiering system administrators with the ability to create or terminate user access. A limitation of the cashiering system is that it does not include an administrator account, one that could be used by a supervisor who does not receive cash, to administer user accounts and access permissions. Failure to segregate system administrator, cashier and cashiering supervisor duties increases the risk of unauthorized changes to cashiering employee user access and data. (Control Finding)

Recommendation No. 2: We recommend the Treasurer reassign the responsibility for user account administration to a supervisor who does not have cash receipt responsibilities.



Treasurer-Tax Collector Response: Concur – Cashier functions are no longer performed by the Cashiering Supervisor. In addition to supervision, the Cashiering Supervisor helps with closing cashiering stations and cash pick-ups. Management is exploring the most appropriate person to fulfill the role of the system administrator and will finalize their decision by October 31, 2006.

Internal Controls Over Granting Network Access

Finding No. 3: An employee no longer requiring Back Office System access has an active user account. Users no longer needing access to the computer system increase the risk of misappropriation of assets. (Control Finding)

Access controls protect against unauthorized entry or use of a computer system. The designated owner of the computer system is responsible for authorizing access to the information with regard to the classification of the information and the need for access to the information.

Recommendation No. 3: We recommend the Treasurer review user accounts for the Back Office System and ensure accounts only exist for active users.

Treasurer-Tax Collector Response: Concur- We removed the names of all non-active user accounts from the Back Office System. Apart from TTC network security, the Back Office System has two layers of security – the application level and the data level. Users have to be listed in both layers before they can use the system. A TTC Information Technology (IT) Analyst adds or deletes users from the Back Office System only through the direction of Back Office User Supervisors. This is communicated through email or User Access Request Form. We implemented a new monthly procedure requiring an IT Analyst to provide each supervisor with a Back Office User Access report listing all users. Supervisors review the report for inactive users, initial it, and keep it on file. This new procedure is effective July 31, 2006.

IT Logical Security Controls

Finding No. 4: The password used to access the Cashiering System, although unique to each user, is static and does not have adequate complexity requirements. The Cashiering System does not require passwords to be of a minimum length or level of complexity (e.g., alpha-numeric) and does not force periodic password changes, thus increasing the risk of unauthorized access. (Control Finding)

Logical security controls are designed to restrict access to computer software and data files. If passwords are used for access control, passwords should consist of at least six to eight alpha numeric characters with no resemblance to any personal data.

Recommendation No. 4: We recommend the Treasurer improve security controls over passwords to access the Cashiering System to require that passwords are at least six to eight alpha numeric characters.

Treasurer-Tax Collector Response: Concur - We have initiated talks with the vendor of the Cashiering System to incorporate this enhancement and have included the necessary funds in our fiscal year 2006-2007 budget to do so. Our IT Division will work with the vendor to upgrade the Cashiering system security to current standards. At this time we do not have a delivery date from the vendor.



Recognizing this weakness, IT has strengthened the TTC network by setting up a more secure password complexity requirement. The following password requirements are now embedded in the TTC Windows policy: Passwords must 1) change every 90 days, 2) have a minimum of six characters, 3) not repeat all or part of the user's name, 4) not repeat the last four passwords used, and 5) comply to at least three of the following categories -- numeric, special character, upper case, and lower case.

IT Security Monitoring Controls

Finding No. 5: User request and approval documentation for changes to the Quantum system are not retained and changes were not documented in a change control log. Not maintaining a change control log with user requests and approval documentation increases the risk of implementing changes not meeting management's business needs, unauthorized changes, and no audit trail. (Control Finding)

Security monitoring controls are critical to data and system integrity. Enhancing information security includes maintaining a record of system changes and visible trail of evidence to trace information contained in reports back to the original input source.

Recommendation No. 5: We recommend the Treasurer require documentation (e.g., user request, vendor correspondence, approvals, etc.) for all changes to the Quantum system be retained and all such changes are documented in a change control log.

Treasurer-Tax Collector Response: Concur - All planned patches and fixes to Quantum are communicated to the users via e-mail. Users, in turn, e-mail their approval of the patch/fix after user testing. Effective June 1, 2006, the IT Analysts have been directed to keep copies of all correspondences pertaining to patches and fixes in a control log, including all recent fixes and changes to Quantum. As an additional audit trail, Quantum automatically maintains all changes in a System Message Log.

Finding No. 6: The Wells Fargo Bank Commercial Electronic Office system's audit trails are maintained on-line for 30 days and not archived by the Treasurer's Office. In addition, the audit report for security activity is not reviewed. Insufficient retention and review of audit trail information increases the risk of not detecting errors and irregularities. (Control Finding)

Recommendation No. 6: We recommend the Treasurer archive a copy of the Wells Fargo Bank Commercial Electronic Office audit report on a monthly basis and perform and document a review of the report for security activity.

Treasurer-Tax Collector Response: Concur – Wells Fargo Bank Commercial Electronic Office (CEO) is comprised of many different products/services. All of the services, except for one, are products created and owned by Wells Fargo Bank. The one exception is Internet ACH. Internet ACH is used for making general ACH payments via the Internet, but also contains a specific module for making various types of tax payments. Due to the intricacies of tax payments, Wells Fargo chose to use an outside vendor for this product. It is a Politzer & Haney product and it functions differently from all the other services on CEO. The audit reports for Wells Fargo products are retained for 365 days and are centralized within a product called Self Administration. The Internet ACH product acts as a stand alone service. Its audit reports are maintained within Internet ACH and are only retained for 30 days. Wells Fargo is currently working toward expanding this retention period.



The Treasurer-Tax Collector has implemented a policy to archive and review audit reports on a monthly basis. These audit reports will include both Self Administration and Internet ACH, thus covering all products contained within CEO. These reports will be created by a CEO administrator – currently the Assistant Cash Manager, Cash Manager or Deputy Treasurer, and will be reviewed by a manager who is not a CEO Administrator. This process is effective for transactions beginning May 1, 2006.

IT Physical Security

Physical security controls involve a plan dealing with exposures and catastrophes. To be effective, the plan should be documented, protect against loss or harm and tested periodically.

Finding No. 7: Back-up procedures for the Treasurer's Local Area Network servers are not documented. The lack of detailed back-up procedures increases the risk of omitting critical steps and loss of financial information. (Control Finding)

Recommendation No. 7: We recommend the Treasurer document detailed procedures for backing up the Local Area Network servers, namely those associated with the Quantum system.

Treasurer-Tax Collector Response: Concur -The TTC has documented the Local Area Network Backup and Restore Procedures in writing.

Finding No. 8: The server room in the Treasurer's Office does not have fire or smoke detection equipment. In addition, the server room does not have an emergency notification system for environmental problems (e.g., failure of air conditioning unit in server room). The absence of smoke detection equipment and environmental controls, increase the risk of damage to the computer room equipment and data due to an inability to respond timely. (Control Finding)

Recommendation No. 8: We recommend the Treasurer evaluate installing fire detection devices and implementing an environmental control problem notification system.

Treasurer-Tax Collector Response: Concur – The TTC will evaluate fire detection devices and assess the feasibility of installing an environmental control problem notification system by December 31, 2006.

Finding No. 9: The Treasurer does not have a documented IT incident response plan. Without a documented incident response plan, the risk of IT staff not understanding their specific roles and responsibilities increases. (Control Finding)

Recommendation No. 9: We recommend the Treasurer document a formal security incident response plan for its IT function. The response plan should include a definition of a security incident, identification of employees to be notified and specific actions to be taken.

Treasurer-Tax Collector Response: Concur - The TTC network administrator, his backup, and IT Analysts review the network logs, Cashiering audit log, and Quantum master audit log daily to ensure that the system has not been compromised. They are directed to report immediately to the IT Manager and examine all necessary reports to effect the necessary changes to the system if there is reason to believe that there is a system breach. The IT Manager will document this procedure in writing by December 31, 2006.



Finding No. 10: The Treasurer has documented a comprehensive disaster recovery plan; however, the plan has not been tested. Testing the plan on a regular basis will help ensure that the IT systems can be effectively recovered, shortcomings are addressed and the plan remains relevant. (Control Finding)

Recommendation No. 10: We recommend the Treasurer test the disaster recovery plan on a regular (annual) basis.

Treasurer-Tax Collector Response: Concur – TTC management will develop a policy and procedure by September 30, 2006, to annually test the department’s disaster recovery plan.

Investment Policy Statement

Finding No. 11: The updated and adopted version of the Investment Policy Statement (IPS) effective for calendar year 2006 removed the Treasurer and members of the Treasury Oversight Committee (TOC) from the list of individuals required to complete on an annual basis the State of California Form 700, Statement of Economic Interests Disclosure. Although the IPS does not provide an exemption from the State Government Code requirement to complete on an annual basis the Statement of Economic Interest, the individuals succeeding the outgoing Treasurer, TOC members, and outside auditors may rely solely on the IPS for guidance. (Control Finding)

Recommendation No. 11: We recommend the Treasurer submit an amended Investment Policy Statement to the Board of Supervisors for consideration showing the Treasurer and Oversight Committee members on the list of individuals required to complete an annual Form 700, Statement of Economic Interest Disclosure.

Treasurer-Tax Collector Response: Do not concur – The Treasurer is specifically called upon to report any material financial interests in the first paragraph of Section VII. The Treasury Oversight Committee is specifically mentioned in the second paragraph, and staff, or “designated employees,” is specifically mentioned by title in the third paragraph. The wording of this section has already been reviewed and approved by County Counsel. However, this concern will be brought to the attention of the Treasurer’s Advisory Committee and the Treasury Oversight Committee at their next scheduled meetings for their review and advisement.



ATTACHMENT A: Report Item Classifications

For purposes of reporting our audit observations and recommendations, we have classified 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:

Audit findings 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.





OFFICE OF THE TREASURER-TAX COLLECTOR

HALL OF FINANCE & RECORDS
12 CIVIC CENTER PLAZA, SUITE G76
POST OFFICE BOX 4515
SANTA ANA, CA 92701
www.ocgov.com/treas

JOHN M.W. MOORLACH, C.P.A., CFP®
TREASURER-TAX COLLECTOR

CHRISS W. STREET
TREASURER-TAX COLLECTOR-ELECT

PAUL C. GORMAN, C.P.A., CTP
DEPUTY TREASURER

WALTER DANIELS
DEPUTY TAX COLLECTOR

ROBIN RUSSELL
DEPUTY TREASURER-TAX COLLECTOR
ADMINISTRATION

CLARISSA ADRIANO-CERES
DEPUTY TREASURER-TAX COLLECTOR
INFORMATION TECHNOLOGY

BRETT R. BARBRE
DEPUTY TREASURER-TAX COLLECTOR
PUBLIC INFORMATION OFFICER

August 24, 2006

Dr. Peter Hughes, CPA
Director, Internal Audit
County of Orange
400 Civic Center Drive West
Building 12, Room 232
Santa Ana, CA 92701-4521

RECEIVED

SEP 22 2006

INTERNAL AUDIT
DEPARTMENT

Dear Dr Hughes:

Pursuant to Audit Oversight Committee Administrative Procedure No. 1, we have prepared our response to the draft results of your Management Letter on Audit of Statement of Assets held by County Treasury as of December 31, 2005. The recommendation numbers used in your report reference our response.

Segregation of Duties

Finding No. 1

The Treasurer utilizes the Wells Fargo Bank Commercial Electronic Office application to send payroll taxes to governing agencies through Automated Clearing House (ACH) transactions. Transaction data is input by one employee, reviewed manually by a second employee, processed/released by the assistant cash manager, and subsequently reconciled by another employee. During our review of roles and responsibilities for the process, it was noted that one employee has an inappropriate combination of user permissions to both edit and release an ACH transaction batch. These incompatible user permissions increase the risk of accidental or unauthorized changes to transactions that could result in the release of fraudulent ACH transactions. (Significant Issue) (**Finding Summary #22**)

Recommendation No. 1

We recommend the Treasurer revoke the employee's permissions to both edit and release transaction batches.

Treasurer-Tax Collector Response:

Concur – The Treasurer-Tax Collector's (TTC) policy is to segregate the duties and the related Wells Fargo Bank Commercial Electronic Office user permissions to edit (or create) and release ACH transactions. The inappropriate combination of permissions occurred when making changes to reassign permissions and duties due to employee terminations. Once notified of the error, steps were taken immediately to make the necessary corrections. In addition, on April 3, 2006, we enabled a new security feature recently implemented by Wells Fargo Bank that prohibits users from creating and releasing the same ACH transactions regardless of individual user permissions.



Page 2 of 7
Peter Hughes
August 24, 2006

Finding No. 2

Two individuals with cashiering and supervisory user access serve as cashiering system administrators with the ability to create or terminate user access. A limitation of the cashiering system is that it does not include an administrator account, one that could be used by a supervisor who does not receive cash, to administer user accounts and access permissions. Failure to segregate system administrator, cashier and cashiering supervisor duties increases the risk of unauthorized changes to cashiering employee user access and data. (Control Finding) (**Finding Summary #6**)

Recommendation No. 2

We recommend the Treasurer reassign the responsibility for user account administration to a supervisor who does not have cash receipt responsibilities.

Treasurer-Tax Collector Response:

Concur - Cashier functions are no longer performed by the Cashiering Supervisor. In addition to supervision, the Cashiering Supervisor helps with closing cashiering stations and cash pick-ups. Management is exploring the most appropriate person to fulfill the role of the system administrator and will finalize their decision by October 31, 2006.

Internal Controls Over Granting Network Access

Finding No. 3:

An employee no longer requiring Back Office System access has an active user account. Users no longer needing access to the computer system increase the risk of misappropriation of assets. (Control Finding) (**Finding Summary #11**)

Recommendation No. 3

We recommend the Treasurer review user accounts for the Back Office System and ensure accounts only exist for active users.

Treasurer-Tax Collector Response:

Concur - We removed the names of all non-active user accounts from the Back Office System. Apart from TTC network security, the Back Office System has two layers of security – the application level and the data level. Users have to be listed in both layers before they can use the system. A TTC Information Technology (IT) Analyst adds or deletes users from the Back Office System only through the direction of Back Office User Supervisors. This is communicated through e-mail or a User Access Request Form. We implemented a new monthly procedure requiring an IT Analyst to provide each supervisor with a Back Office User Access report listing all users. Supervisors review the report for inactive users, initial it, and keep it on file. This new procedure is effective July 31, 2006.



Page 3 of 7
Peter Hughes
August 24, 2006

IT Logical Security Controls

Finding No. 4

The password used to access the Cashiering System, although unique to each user, is static and does not have adequate complexity requirements. The Cashiering System does not require passwords to be of a minimum length or level of complexity (e.g., alpha-numeric) and does not force periodic password changes, thus increasing the risk of unauthorized access. (Control Finding) (**Finding Summary #8**)

Logical security controls are designed to restrict access to computer software and data files. If passwords are used for access control, passwords should consist of at least six to eight alpha-numeric characters with no resemblance to any personal data.

Recommendation No. 4

We recommend the Treasurer improve security controls over passwords to access the Cashiering System to require that passwords are at least six to eight alpha numeric characters.

Treasurer-Tax Collector Response:

Concur - We have initiated talks with the vendor of the Cashiering System to incorporate this enhancement and have included the necessary funds in our fiscal year 2006-2007 budget to do so. Our IT Division will work with the vendor to upgrade the Cashiering system security to current standards. At this time we do not have a delivery date from the vendor.

Recognizing this weakness, IT has strengthened the TTC network by setting up a more secure password complexity requirement. The following password requirements are now embedded in the TTC Windows policy: Passwords must 1) change every 90 days, 2) have a minimum of six characters, 3) not repeat all or part of the user's name, 4) not repeat the last four passwords used, and 5) comply to at least three of the following categories -- numeric, special character, upper case, and lower case.

IT Security Monitoring Controls

Finding No. 5

User request and approval documentation for changes to the Quantum system are not retained and changes were not documented in a change control log. Not maintaining a change control log with user requests and approval documentation increases the risk of: implementing changes not meeting management's business needs; unauthorized changes; and no audit trail. (Control Finding) (**Finding Summary #5**)

Security monitoring controls are critical to data and system integrity. Enhancing information security includes maintaining a record of system changes and visible trail of evidence to trace information contained in reports back to the original input source.



Page 4 of 7
Peter Hughes
August 24, 2006

Recommendation No. 5

We recommend the Treasurer require documentation (e.g., user request, vendor correspondence, approvals, etc.) for all changes to the Quantum system be retained and all such changes are documented in a change control log.

Treasurer-Tax Collector Response:

Concur - All planned patches and fixes to Quantum are communicated to the users via e-mail. Users, in turn, e-mail their approval of the patch/fix after user testing. Effective June 1, 2006, the IT Analysts have been directed to keep copies of all correspondences pertaining to patches and fixes in a control log, including all recent fixes and changes to Quantum. As an additional audit trail, Quantum automatically maintains all changes in a System Message Log.

Finding No. 6

The Wells Fargo Bank Commercial Electronic Office system's audit trails are maintained on-line for 30 days and not archived by the Treasurer's Office. In addition, the audit report for security activity is not reviewed. Insufficient retention and review of audit trail information increases the risk of not detecting errors and irregularities. (Control Finding) **(Finding Summary #23)**

Recommendation No. 6

We recommend the Treasurer archive a copy of the Wells Fargo Bank Commercial Electronic Office audit report on a monthly basis and perform and document a review of the report for security activity.

Treasurer-Tax Collector Response:

Concur – Wells Fargo Bank Commercial Electronic Office (CEO) is comprised of many different products/services. All of the services, except for one, are products created and owned by Wells Fargo Bank. The one exception is Internet ACH. Internet ACH is used for making general ACH payments via the Internet, but also contains a specific module for making various types of tax payments. Due to the intricacies of tax payments, Wells Fargo chose to use an outside vendor for this product. It is a Politzer & Haney product and it functions differently from all the other services on CEO. The audit reports for Wells Fargo products are retained for 365 days and are centralized within a product called Self Administration. The Internet ACH product acts as a stand alone service. Its audit reports are maintained within Internet ACH and are only retained for 30 days. Wells Fargo is currently working toward expanding this retention period.

The Treasurer-Tax Collector has implemented a policy to archive and review audit reports on a monthly basis. These audit reports will include both Self Administration and Internet ACH, thus covering all products contained within CEO. These reports will be created by a CEO administrator – currently the Assistant Cash Manager, Cash Manager or Deputy Treasurer, and will be reviewed by a manager who is not a CEO Administrator. This process is effective for transactions beginning May 1, 2006.



Page 5 of 7
Peter Hughes
August 24, 2006

IT Physical Security

Finding No. 7

Back-up procedures for the Treasurer's Local Area Network servers are not documented. The lack of detailed back-up procedures increases the risk of omitting critical steps and loss of financial information. (Control Finding) (**Finding Summary #13**)

Recommendation No. 7

We recommend the Treasurer document detailed procedures for backing up the Local Area Network servers, namely those associated with the Quantum system.

Treasurer-Tax Collector Response:

Concur - The TTC has documented the Local Area Network Backup and Restore Procedures in writing.

Finding No. 8

The server room in the Treasurer's Office does not have fire or smoke detection equipment. In addition, the server room does not have an emergency notification system for environmental problems (e.g., failure of air conditioning unit in server room). The absence of smoke detection equipment and environmental controls increase the risk of damage to the computer room equipment and data due to an inability to respond timely. (Control Finding) (**Finding Summary #14**)

Recommendation No. 8

We recommend the Treasurer evaluate installing fire detection devices and implementing an environmental control problem notification system.

Treasurer-Tax Collector Response:

Concur – The TTC will evaluate fire detection devices and assess the feasibility of installing an environmental control problem notification system by December 31, 2006.

Finding No. 9

The Treasurer does not have a documented IT incident response plan. Without a documented incident response plan, the risk of IT staff not understanding their specific roles and responsibilities increases. (Control Finding) (**Finding Summary #12**)

Recommendation No. 9

We recommend the Treasurer document a formal security incident response plan for its IT function. The response plan should include a definition of a security incident, identification of employees to be notified and specific actions to be taken.



Page 6 of 7
Peter Hughes
August 24, 2006

Treasurer-Tax Collector Response:

Concur - The TTC network administrator, his backup, and IT Analysts review the network logs, Cashiering audit log, and Quantum master audit log daily to ensure that the system has not been compromised. They are directed to report immediately to the IT Manager and examine all necessary reports to effect the necessary changes to the system if there is reason to believe that there is a system breach. The IT Manager will document this procedure in writing by December 31, 2006.

Finding No. 10

The Treasurer has documented a comprehensive disaster recovery plan; however, the plan has not been tested. Testing the plan on a regular basis will help ensure that the IT systems can be effectively recovered, shortcomings are addressed and the plan remains relevant. (Control Finding) (**Finding Summary #7**)

Recommendation No. 10

We recommend the Treasurer test the disaster recovery plan on a regular (annual) basis.

Treasurer-Tax Collector Response: Concur – TTC management will develop a policy and procedure by September 30, 2006, to annually test the department's disaster recovery plan.

Investment Policy Statement

Finding No. 11

The updated and adopted version of the Investment Policy Statement (IPS) effective for calendar year 2006 removed the Treasurer and members of the Treasury Oversight Committee (TOC) from the list of individuals required to complete on an annual basis the State of California Form 700, Statement of Economic Interests Disclosure. Although the IPS does not provide an exemption from the State Government Code requirement to complete on an annual basis the Statement of Economic Interest, the individuals succeeding the outgoing Treasurer, TOC members, and outside auditors may rely solely on the IPS for guidance. (Control Finding) (**Finding Summary #21**)

Recommendation No. 11

We recommend the Treasurer submit an amended Investment Policy Statement to the Board of Supervisors for consideration showing the Treasurer and Oversight Committee members on the list of individuals required to complete an annual Form 700, Statement of Economic Interest Disclosure.



Page 7 of 7
Peter Hughes
August 24, 2006

Treasurer-Tax Collector Response:

Do not concur - The Treasurer is specifically called upon to report any material financial interests in the first paragraph of Section VII. The Treasury Oversight Committee is specifically mentioned in the second paragraph, and staff, or "designated employees," is specifically mentioned by title in the third paragraph. The wording of this section has already been reviewed and approved by County Counsel. However, this concern will be brought to the attention of the Treasurer's Advisory Committee and the Treasury Oversight Committee at their next scheduled meetings for their review and advisement.

If you have additional questions or follow-up comments, please contact Paul Gorman, Deputy Treasurer at 834-2288.

Very truly yours,



John M. W. Moorlach, C.P.A., CFP®
Orange County Treasurer-Tax Collector

