GOVERNMENT OF THE DISTRICT OF COLUMBIA
OFFICE OF THE INSPECTOR GENERAL

APPLICATION CONTROL REVIEW OF THE INTEGRATED TAX SYSTEM

CHARLES J. WILLOUGHBY
INSPECTOR GENERAL

OIG No. 11-1-11AT

May 15, 2013

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Office of the Inspector General

Inspector General

May 15, 2013

Natwar M. Gandhi, Ph.D.
Chief Financial Officer
Office of the Chief Financial Officer
The John A. Wilson Building
1350 Pennsylvania Avenue, N.W. Suite 203
Washington, D.C. 20004

Dear Dr. Gandhi:

Enclosed is the final report summarizing the results of the Office of the Inspector General's (OIG) *Application Control Review of the Integrated Tax System* (OIG No. 11-1-11AT). The audit was included in the OIG's Fiscal Year 2011 Audit and Inspection Plan.

As a result of our audit, we directed 18 recommendations to the Office of the Chief Financial Officer (OCFO) for action we consider necessary to correct identified deficiencies. OCFO provided a written response to the draft of this report on April 5, 2013. The full text of OCFO's response is included at Exhibit B.

OCFO actions taken or planned for Recommendations 1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 13, 16, and 18 are considered responsive and meet the intent of the recommendations. However, OCFO did not provide target dates for completing the planned actions for Recommendations 8, 10, 13, and 16. Thus, we request that OCFO provide estimated completion dates for these four recommendations within 60 days of the date of this final report.

OCFO did not concur with Recommendations 9, 11, and 17. Additionally, OCFO responses to Recommendations 14, and 15 did not fully meet the intent of the recommendation and remain unresolved. Accordingly, we respectfully request that OCFO reconsider its position taken on these five recommendations and provide our Office with a revised response within 60 days of the date of this final report.

This report has cleared the OIG disclosure review process and information determined to be restricted from public release has been omitted from this document pursuant to *Government Auditing Standards* (2007 Rev.) Paragraph 8.38, Reporting Confidential or Sensitive Information, issued by the Comptroller General of the United States. In this regard, one finding and recommendation related to IT security has been presented to your Office in a separate letter due to the sensitive nature of the information.

We appreciate the cooperation and courtesies extended to our staff by the OCFO personnel. If you have questions concerning this report, please contact me or Ronald King, Assistant Inspector General for Audits, at (202) 727-2540.

Sincerely,

Charles J. Willoughby

Charles J. Willoughby
Inspector General

CJW/rjb

Enclosure

cc: See Distribution List

DISTRIBUTION:

The Honorable Vincent C. Gray, Mayor, District of Columbia
Mr. Allen Y. Lew, City Administrator, District of Columbia (via email)
Mr. Victor L. Hoskins, Deputy Mayor for Planning and Economic Development, District of Columbia (via email)
The Honorable Phil Mendelson, Chairman, Council of the District of Columbia (via email)
The Honorable Kenyan McDuffie, Chairperson, Committee on Government Operations, Council of the District of Columbia (via email)
The Honorable Jack Evans, Chairman, Committee on Finance and Revenue, Council of the District of Columbia (via mail)
Mr. Brian Flowers, General Counsel to the Mayor (via email)
Mr. Christopher Murphy, Chief of Staff, Office of the Mayor (via email)
Ms. Janene Jackson, Director, Office of Policy and Legislative Affairs (via email)
Mr. Pedro Ribeiro, Director, Office of Communications, (via email)
Mr. Eric Goulet, Budget Director, Mayor’s Office of Budget and Finance
Ms. Nyasha Smith, Secretary to the Council (1 copy and via email)
Mr. Irvin B. Nathan, Attorney General for the District of Columbia (via email)
Dr. Natwar M. Gandhi, Chief Financial Officer (via email)
Mr. Mohamad Yusuff, Interim Executive Director, Office of Integrity and Oversight, Office of the Chief Financial Officer (via email)
Ms. Yolanda Branche, D.C. Auditor
Mr. Phillip Lattimore, Director and Chief Risk Officer, Office of Risk Management (via email)
Mr. Steve Sebastian, Managing Director, FMA, GAO, (via email)
The Honorable Eleanor Holmes Norton, D.C. Delegate, House of Representatives, Attention: Bradley Truding (via email)
The Honorable Darrell Issa, Chairman, House Committee on Oversight and Government Reform, Attention: Howie Denis (via email)
The Honorable Elijah Cummings, Ranking Member, House Committee on Oversight and Government Reform, Attention: Yvette Cravins (via email)
The Honorable Thomas Carper, Chairman, Senate Committee on Homeland Security and Governmental Affairs, Attention: Holly Idelson (via email)
The Honorable Tom Coburn, Ranking Member, Senate Committee on Homeland Security and Governmental Affairs, Attention: Katie Bailey (via email)
The Honorable Mark Begich, Chairman, Senate Subcommittee on Emergency Management, Intergovernmental Relations and the District of Columbia, Attention: Cory Turner (via email)
The Honorable Rand Paul, Ranking Member, Senate Subcommittee on Emergency Management, Intergovernmental Relations and the District of Columbia
The Honorable Harold Rogers, Chairman, House Committee on Appropriations, Attention: Amy Cushing (via email)
The Honorable Nita Lowey, Ranking Member, House Committee on Appropriations, Attention: Laura Hogshead (via email)
The Honorable Ander Crenshaw, Chairman, House Subcommittee on Financial Services and General Government, Attention: Amy Cushing (via email)

The Honorable José E. Serrano, Ranking Member, House Subcommittee on Financial Services and General Government, Attention: Laura Hogshead (via email)
The Honorable Barbara Mikulski, Chairwoman, Senate Committee on Appropriations, Attention: Ericka Rojas (via email)
The Honorable Richard Shelby, Ranking Member, Senate Committee on Appropriations, Attention: Dana Wade (via email)
The Honorable Frank Lautenberg, Chairman, Senate Subcommittee on Financial Services and General Government, Attention: Marianne Upton (via email)
The Honorable Mike Johanns, Ranking Member, Senate Subcommittee on Financial Services and General Government, Attention: Dale Cabaniss (via email)

ACRONYMS

ASA	Application Security Administrator
CAFR	Comprehensive Annual Financial Report
CAMA	Computer Assisted Mass Appraisal
CIO	Chief Information Officer
COTS	Commercial Off the Shelf
COBIT	Control Objectives for Information and related Technology
CSA	Customer Service Administration
CTS	Correspondence Tracking System
CY	Calendar Year
DCMR	District of Columbia Municipal Regulations
e-file	Electronically File
eTSC	Electronic Taxpayer Service Center
FY	Fiscal Year
IDCS	Integrated Data Capture System
IT	Information Technology
ITS	Integrated Tax System
MITS	Modern Integrated Tax System
MRPTS	Modern Real Property Tax System
OAG	Office of the Attorney General
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OCTO	Office of the Chief Technology Officer
OIG	Office of the Inspector General

ACRONYMS (continued)

OTR	Office of Tax and Revenue
RSI	Revenue Solutions, Inc.
SDLC	Systems Development Life Cycle
SOAR	System of Accounting and Reporting
SOD	Segregation of Duties
TAS	Tax Administration System
TBD	To Be Determined
TSG	Tax Systems Group
TY	Tax Year

TABLE OF CONTENTS

EXECUTIVE SUMMARY

OVERVIEW

The District of Columbia Office of the Inspector General (OIG) has completed an *Application Control Review of the Integrated Tax System.* This audit was included in the Office of the Inspector General's *Fiscal Year 2011 Audit and Inspection Plan*.

The District of Columbia Office of Tax and Revenue (OTR), which operates under the authority of the Office of the Chief Financial Officer (OCFO), is responsible for administrating the District's business, income, excise, and real property tax laws. To facilitate and support OTR's mission, management decided to implement the Integrated Tax System (ITS) in 1999. The Office of the Chief Information Officer (OCIO) handles the maintenance and modification of ITS in response to the changing needs of OTR.

Our audit objectives were to: (1) assess the efficiency and effectiveness of the design and operation of the ITS; and (2) evaluate the effectiveness of internal controls established and implemented to adequately safeguard against fraud, waste, and abuse.

CONCLUSIONS

OTR lacked adequate management controls to ensure that: (1) sufficient and effective governance tools were formally developed to better direct information technology (IT) expenditures for optimal advantage and risk management; (2) risks associated with the delivery and support of software applications were sufficiently mitigated; and (3) application and general controls were aligned with applicable statutory provisions and best practices to minimize the risk of errors and fraud.

As a result, OTR failed to collect $6.5 million in penalty revenue and adequately minimize the risk of tax fraud and errors. Moreover, the conditions found during this audit further revealed that OTR is at risk of: (1) unnecessary or wasteful spending related to inefficient resource management and inadequate planning; (2) insufficient application support; and (3) unauthorized changes to critical data and programs. These and other matters requiring management's attention are detailed in the following sections of this report.

SUMMARY OF RECOMMENDATIONS

We directed 18 recommendations to OCFO that we believe are necessary to address deficiencies identified during the audit. The recommendations focus on: (1) developing an IT strategic plan aligned with the agency's strategic objectives; (2) adopting a well-established IT governance model to integrate good business practices in service delivery functions; and (3) strengthening application and general controls related to the ITS and the District's tax administration processes.

This report has cleared the OIG disclosure review process and information determined to be restricted from public release has been omitted from this document pursuant to *Government*

EXECUTIVE SUMMARY

Auditing Standards (2007 Rev.) Paragraph 8.38, Reporting Confidential or Sensitive Information, issued by the Comptroller General of the United States. In this regard, one finding and recommendation related to IT security has been presented to OCFO in a separate letter due to the sensitive nature of the information and potential security risk.

A summary of potential benefits resulting from this audit is included at Exhibit A.

MANAGEMENT RESPONSE AND OIG COMMENTS

On April 5, 2013, OCFO provided a written response to the draft of this report. OCFO actions taken or planned for Recommendations 1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 13, 16, and 18 are considered responsive and meet the intent of the recommendations. However, OCFO did not provide target dates for completing the planned actions for Recommendations 8, 10, 13, and 16. Thus, we request that OCFO provide estimated completion dates for these four recommendations within 60 days of the date of this final report.

OCFO did not concur with Recommendations 9, 11, and 17. Additionally, OCFO responses to Recommendations 14, and 15 did not fully meet the intent of the recommendation and remain unresolved. Accordingly, we respectfully request that OCFO reconsider its position taken on these five recommendations and provide our Office with a revised response within 60 days of the date of this final report. The full text of the OCFO response is included at Exhibit B.

INTRODUCTION

BACKGROUND

This audit was included in the Office of the Inspector General's (OIG) *Fiscal Year 2011 Audit and Inspection Plan*. The purpose of the audit was to examine the adequacy and effectiveness of controls over the District's tax processing procedures related to the Integrated Tax System (ITS). This audit was prompted by frauds perpetrated by District government employees who exploited vulnerabilities in and around the ITS.

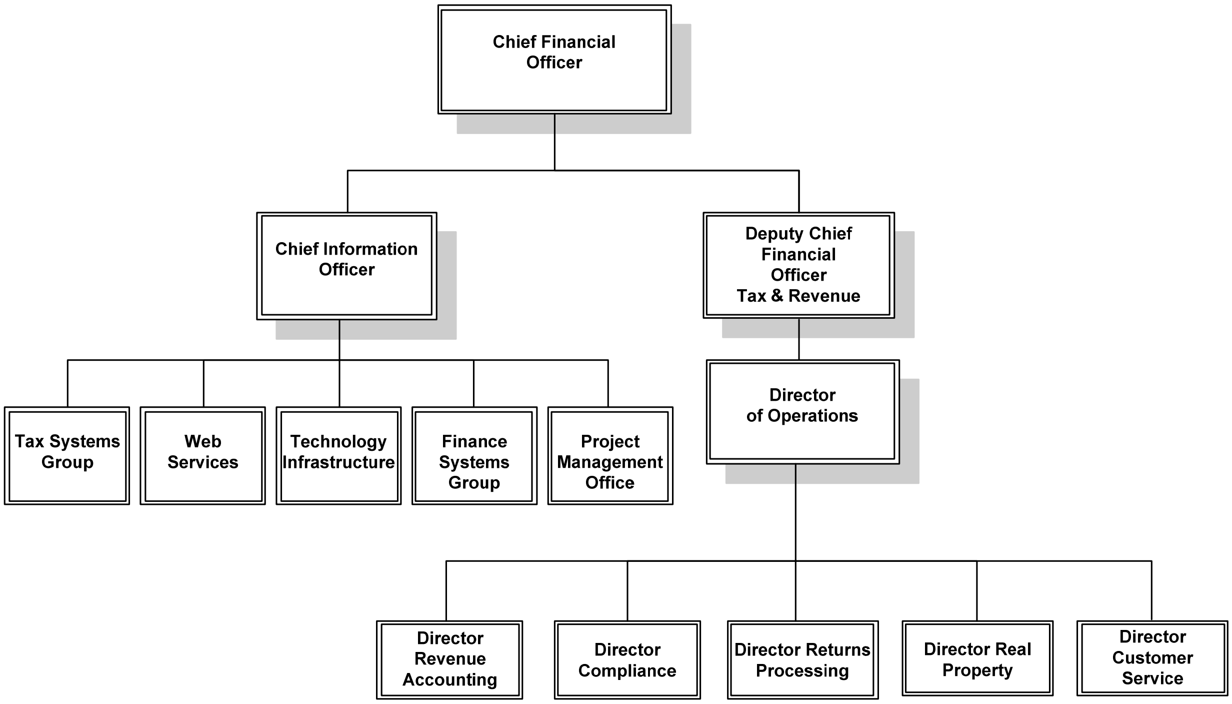
The ITS is the District's system for processing tax returns, including individual income taxes, real property taxes, and various business taxes. The system's processes are owned by the Office of Tax and Revenue (OTR), which is a department under the Office of the Chief Financial Officer (OCFO). (See Page 2, Figure 1.)

The mission of the OCFO is to enhance the fiscal and financial stability, accountability, and integrity of the District government. OCFO is responsible for:

- oversight of the financial and budgetary functions of the District government;
- operating and maintaining a coordinated financial management system to budget, collect, control, and properly account for more than $7 billion in annual operating and capital funds;
- preparing the District's annual budget, representing the District in the federal appropriations process, and monitoring budget performance during the fiscal year;
- borrowing on behalf of the District, collecting receipts, payments, and transactions for the District, and investing the District's funds;
- administering and enforcing the District's tax laws, collecting revenue for the District, and recording deeds and other written instruments affecting a right, title, or interest in real or personal property in the District;
- developing, implementing, and monitoring the District's accounting policies and systems, and producing the audited Comprehensive Annual Financial Report (CAFR) for the District; and
- forecasting revenue for the District government, developing fiscal impact statements for proposed legislation, performing tax expenditure analysis, and providing advice on economic development matters.

INTRODUCTION

Figure 1. Excerpt of the Office of the Chief Financial Officer Organizational Chart Relative to the Office of Tax and Revenue


Chief Financial Officer
Chief Information Officer
Deputy Chief Financial Officer Tax & Revenue
Tax Systems Group
Web Services
Technology Infrastructure
Finance Systems Group
Project Management Office
Director of Operations
Director Revenue Accounting
Director Compliance
Director Returns Processing
Director Real Property
Director Customer Service

OTR is the primary user of the ITS. OTR's mission is to collect the proper amount of tax owed to the District government and correctly account for all revenue, while minimizing the burden on taxpayers and the cost to the government. The ITS is maintained and modified by the Tax Systems Group (TSG), a designated team within the Office of the Chief Information Officer (OCIO), which supports IT services for the entire OCFO. (See Figure 1 above.) TSG is managed by OCIO employees with many of the application development and support services being outsourced to a third-party contractor.

The District purchased the ITS from Accenture Ltd. (Accenture) and implemented it in phases, beginning with business taxes in November 2000. Accenture provided third-party support services since the implementation of the ITS, until the contract was awarded to Revenue Solutions, Inc. (RSI) in February 2009. The RSI contract term was for 1 year, with 4 additional option years, and the contract is currently in the 4th option year.

OTR is in the process of replacing the ITS with one or more integrated commercial off the shelf (COTS) software products, and expects to implement the Modern Integrated Tax System (MITS) and Modern Real Property Tax System (MRPTS) within the next 3 to 5 years.

INTRODUCTION

SYSTEM DESCRIPTIONS

Integrated Tax System (ITS) – An enterprise-wide tax processing, remittance deposit, posting, and tracking system with electronic and web-based facilities. The system utilizes a combination of customized and proprietary software. In addition to the core ITS functions, other system components include imaging and data capture, reporting, customer relationship management, correspondence, real property, data warehouse, and an enterprise service bus.[1] The ITS supports the administration of the District's various tax types, including personal income, business, and real property taxes.

Tax Administration System (TAS) – The financial accounting module for the ITS, which provides returns processing, taxpayer accounting, billing, refunding, collections processing, and revenue accounting. The system was created to give program owners, managers, users, and executives information related to the collection, maintenance, and administration of taxes. The system is designed to support analysts who have a need to conduct research about various tax administration initiatives, or who wish to measure the success of their program.

Computer Assisted Mass Appraisal (CAMA) – This system supports all real property appraisal functions, including the annual reevaluation of residential and commercial properties. It is a client-server application that maintains property attributes, photos, assessments, and sketches. The CAMA system has an indirect interface to the TAS mainframe to upload property and tax-related information and download property and tax-related updates that occur in TAS.

Electronic Taxpayer Service Center (eTSC) – This system allows District of Columbia businesses and individuals to report and pay their tax obligations using the Internet. Individuals and registered businesses can file tax returns; submit electronic payments; view account balance information; view OTR correspondence; and submit questions to OTR. The data is transferred nightly from eTSC to TAS where the returns are processed.

Integrated Data Capture System (IDCS) – This system provides the data capture and imaging functions for the ITS that are performed at OTR. The majority of the imaging and payment processing (70-75 percent) is outsourced to the Lockbox, which includes two, third-party vendors contracted by OTR to scan, data capture, and image returns and payments. The IDCS supports the scanning, imaging, data capture, check encoding, data repair, data review, and payment balancing processes for the District's paper tax returns imaged at OTR.

[1] An enterprise service bus is a flexible connectivity infrastructure that effectively allows communication between applications and services.

INTRODUCTION

CRITERIA

The statutes, regulations, policies, and procedures related to this audit include the following:

- D.C. Code § 47-4402(c) (Supp. 2011), Credit Card or Electronic Payment of Taxes.
- General Requirements for Filing Tax Returns Including Electronic [Internet] Filing, 9 DCMR § 105.
- D.C. Code § 47-1812.08 (Supp. 2011), Withholding of Tax.
- D.C. Code § 1-1403 (Supp. 2011), Functions of the Office of the Chief Technology Officer.
- District of Columbia Office of the Chief Financial Officer Financial Policies and Procedures Manual.
- Office of Tax and Revenue Policies and Procedures Manuals for each Administration, respectively: Deputy Chief Financial Officer, Revenue Accounting Administration, Compliance Administration, Returns Processing Administration, Real Property Tax Administration, and Customer Service Administration.
- Government of the District of Columbia Office of the Chief Financial Officer Office of the Chief Information Officer Policy/Process Documents.
- Government of the District of Columbia Office of the Chief Technology Officer Information Security Program.

In addition to the above criteria, we relied on ISACA's[2] Control Objectives for Information and related Technology (COBIT) 4.1, 2007. COBIT is an internationally recognized framework that defines best practices for IT governance and control.

[2] ISACA is the single international source for IT controls. It provides practical guidance, benchmarks, and other effective tools for all enterprises that use information systems. Through its comprehensive guidance and services, ISACA defines the roles of information systems governance, security, audit, and assurance professionals worldwide.

INTRODUCTION

OBJECTIVES, SCOPE, AND METHODOLOGY

Our audit objectives were to: (1) assess the efficiency and effectiveness of the design and operation of the ITS; and (2) evaluate the effectiveness of internal controls established and implemented to adequately safeguard against fraud, waste, and abuse.

The ITS is comprised of many applications, databases, platforms, and interfaces. The scope of this audit was limited to TAS, CAMA, eTSC, and IDCS, which are applications used to process the largest revenue-generating individual, business, and real property taxes in the District. The scope was further narrowed to exclude general controls testing in TAS, which is performed annually during the CAFR audit, to prevent overlap between KPMG LLP[3] and OIG audit efforts. We only performed a general control review on the IDCS because it was determined to be a low risk application as the majority of the data capture and imaging is performed by two, third-party contractors.

Our review covered tax administration during the period of March 15, 2011, through April 2, 2012. We accomplished our audit objectives using the following methodology in gathering data and conducting tests:

- Interviewed responsible OCFO, OCIO, and OTR managers and employees to obtain a general understanding of the processes used for managing and monitoring the District's tax assessment and collection processes.

- Met with OCIO and OTR managers and employees to obtain and review financial records, property records, tax returns, source documents, case law, and electronic reports related to tax administration and/or the ITS.

- Reviewed applicable laws and regulations governing the administration, collection, and assessment of taxes and associated penalties for noncompliance.

- Obtained and reviewed copies of policies and procedures governing the administration and monitoring of the District's taxation processes, including IT.

- Reviewed the tax assessment and collection process and documentation maintained by OCFO, OCIO, and OTR.

- Evaluated the adequacy of general and application controls related to the ITS, as well as key processes in tax administration including refunds, penalty assessment and collection, returns processing, and real property tax assessment.

[3] KPMG LLP is the external audit agency currently contracted by the District of Columbia government to perform the annual CAFR audit.

- Reviewed prior audits related to the District's tax administration processes and obtained implementation status updates on those audit recommendations specifically related to the ITS and IT governance.

- Reviewed other relevant documentation as necessary.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

RESULTS OF PRIOR INDEPENDENT AUDITS

In the past 5 years, several independent audits were conducted at OTR. The audit objectives focused on operational, financial, and compliance matters associated with the tax administration processes. We reviewed these audit reports to identify findings and recommendations relevant to our current audit objectives and found the following audit reports with findings related to internal controls and IT-related matters:

***Report on the Office of the Chief Financial Officer's Office of Tax and Revenue – Real Property Tax Refund Process*, issued by Kroll Associates, Inc. on March 5, 2008.** The objectives of this limited review, performed in response to a request by the OCFO after it was notified by federal authorities of potential improprieties within OCFO's OTR, were to independently assess the internal control failures that allowed the real property tax refund fraud discovered in 2007 and evaluate the mitigating controls established. Relevant findings included:

- high volume of manual processing in ITS and SOAR, which increases the potential for error;
- policies and procedures were not properly documented;
- inadequate review and approval process;
- inadequate security controls;
- information systems were not integrated;
- system "change reports" were not generated and/or reviewed;
- real Property Tax Administration employed many manual processes and external databases for functionality; and
- no documented IT strategy that addresses resource requirements, ongoing and future project needs, staffing requirements, training, and related IT support activities.

***Report of Investigation*, issued by Wilmer Cutler Pickering Hale and Dorr LLP in December 2008.** In December 2007, the Council of the District of Columbia established the Office of Tax and Revenue Investigation Special Committee to investigate the facts surrounding the real property tax refund fraud discovered earlier in 2007. This committee retained the law

INTRODUCTION

firm of Wilmer Cutler Pickering Hale and Dorr LLP, which sought the forensic accounting and information technology services of PricewaterhouseCoopers LLP to assist with this investigation. Relevant findings included:

- lack of effective automated controls for manually processed refunds;
- insufficient controls surrounding the creation, modification, or deletion of credit on accounts in ITS;
- ITS lacked controls requiring credits to be compared to actual payments; and
- no audit trail for who initiated, modified, and approved transactions maintained.

***Audit of the Office of the Chief Financial Officer's Implementation of Recommendations Contained in the Wilmer Cutler Pickering Hale and Dorr LLP Report of Investigation*, issued by the District of Columbia Office of the Inspector General (OIG No. 09-02-11AT) on December 9, 2009.** This audit report was in response to a request by the Council of the District of Columbia for a follow-up audit to determine what corrective actions OCFO took to address the recommendations in the investigations report by the Wilmer Cutler Pickering Hale and Door LLP. The OIG found:

- OCFO did not formally identify and evaluate the findings and recommendations contained in the report, or develop a comprehensive and consolidated corrective action plan until after the inception of the OIG audit;
- OCFO had not identified a mechanism for assessing whether corrective actions taken by responsible division managers were appropriate for the recommendations; and
- Of the 62 recommendations that the OIG reviewed (out of 94 in the report), OCFO's management responses and activities met the intent of 60 of the recommendations. Of those 60 recommendations, implementation activities were ongoing for 46 and completed for 14.

***Independent Auditors' Report on Internal Control and Compliance Over Financial Reporting Fiscal Year Ended September 30, 2009*, (OIG No. 10-1-03MA)** issued by BDO Seidman, LLP on February 2, 2010, in conjunction with the District's CAFR audit. The CAFR auditors found:

- access authorization issues in TAS;
- inadequate control over unidentified taxpayer accounts;
- no reconciliation between Real Property Tax Administration and Adjustment Unit and proof of payments;
- inadequate control over the release and re-issuance of the suppressed tax refund;
- no standard operating procedures for downloading and reviewing unpaid taxpayer liabilities from ITS; and
- withholding payments received by the District from employers or taxpayers are not matched to tax payments reported on tax returns.

INTRODUCTION

Independent Auditors' Report on Internal Control and Compliance Over Financial Reporting Fiscal Year Ended September 30, 2010, **(OIG No. 11-1-06MA)** issued by KPMG, LLP on February 11, 2011, in conjunction with the District's CAFR audit. The CAFR auditors found:

- insufficient monitoring of internal control by Returns Processing Administration at its lockbox service provider;
- lack of segregation of duties (SOD) among auditors with the responsibility of preparing assessment adjustments and those that enter adjustments into the ITS;
- insufficient control procedures over the reconciliation of tax withholdings;
- nine of 25 real property tax exemption applications were not properly signed by an assessment specialist; and
- management did not perform adequate verification and validation procedures for setting the allowance for collectible accounts.

FINDINGS AND RECOMMENDATIONS

FINDING 1: INFORMATION TECHNOLOGY STRATEGIC PLAN

SYNOPSIS

Our audit found that the OCIO has not: (1) formally developed and documented an IT strategic plan to coordinate and align the agency's strategic goals with IT expenditures; and (2) created a comprehensive IT applications inventory detailing each application and how it supports the agency's mission. OCIO management could not tell us why these IT governance tools have not been developed. We believe that the lack of formal IT governance standards, policies, and procedures, and management's failure to fully remediate previous audit findings contributed to these conditions. IT governance standards provide a framework of principles on the effective and efficient management of IT resources. As a result, OTR is at risk of unnecessary or wasteful spending because its decisions may not be cohesive and proactive. We believe that these governance tools would enable OTR to leverage their current IT investments and improve their internal business processes.

DISCUSSION

The OCIO does not have a documented IT strategic plan. This condition was previously noted in the independent audit report issued by Kroll in 2008. The Chief Information Officer (CIO) considered this finding "Closed" because the OCIO completed a 2009 IT strategic plan. However, when the OIG audit team requested a copy of the plan, OCIO management could not locate and submit the documentation for our review. In response to Kroll's recommendation, OCIO created an IT steering committee composed of OCFO, OCIO, and OTR managers who hold bi-weekly meetings to discuss IT priorities. OTR management advised that the purpose of these meetings is to assess IT risks associated with tax processing and to prioritize tax system modifications and enhancements. While an IT steering committee is essential to the IT control framework according to COBIT, a formal document aligning IT investments to business requirements is preferred and necessary to balance short-term and long-term business needs.

COBIT Section PO4.3 states that an organization should:

> Establish an IT steering committee (or equivalent) composed of executive, business and IT management to:
>
> - determine prioritisation[4] of IT-enabled investment programmes[5] in line with the enterprise's business strategy and priorities
> - track status of projects and resolve resource conflict

[4] British English spelling.
[5] *Id.*

- monitor service levels and service improvements

Additionally, COBIT Section PO4.2 states that an organization should:

> Establish an IT strategy committee at the board level. This committee should ensure that IT governance, as part of enterprise governance, is adequately addressed; advise on strategic direction; and review major investments on behalf of the full board.

Initially, we requested that OTR provide its departmental strategic plan to determine whether OCIO's IT strategic plan was aligned to OTR's business objectives. In response to this request, OTR provided a presentation entitled "District of Columbia Office of Tax and Revenue FY 2006-2007 Strategic Plan." However, we determined that the plan was outdated and not relevant in evaluating proper alignment to an established IT strategic plan. While OTR's mission may not change, its goals and objectives may evolve and, therefore, must be updated periodically in order to be an effective governance tool.

The OIG requested the OCIO's IT strategic plan for review. In response, OCIO management provided a copy of its 2010 Software Development Life Cycle[6] (SDLC). An SDLC is not a substitute for a formal IT strategic plan. This document is procedural, consisting of a plan for a development team to develop, maintain, and replace specific software, as opposed to identifying and planning IT strategic initiatives.

The *District of Columbia, Office of the Chief Financial Officer, Office of Tax and Revenue, Software Development Life Cycle* consists of the following software management processes adopted by the Tax Systems Group (TSG) that supports the systems used by OTR:

- introduction of TSG;
- requirements to initiate a system change;
- development process;
- quality assurance process;
- operations process; and
- alternate SDLC paths.

The IT strategic plan should include strategies, objectives, budget projections and allocations, and methods for measuring performance. Specifically, COBIT Section PO4.1 provides that an organization:

[6] A software development life cycle, also referred to as a systems development life cycle, is an IT process model that depicts phases deployed in the development or acquisition of a software system. Typical phases include the feasibility study, requirements study, requirements definition, detailed design, programming, testing, installation and post-implementation review.

FINDINGS AND RECOMMENDATIONS

> Define an IT process framework to execute the IT strategic plan. This framework should include an IT process structure and relationships (e.g., to manage process gaps and overlaps), ownership, maturity, performance measurement, improvement, compliance, quality targets, and plans to achieve them. It should provide integration amongst the processes that are specific to IT, enterprise portfolio management, business processes, and business change processes. The IT process framework should be integrated into a quality management system (QMS) and the internal control framework.

Additionally, COBIT Section PO1.4 provides that an organization:

> Create a strategic plan that defines, in co-operation with relevant stakeholders, how IT goals will contribute to the enterprise's strategic objectives and related costs and risks. It should include how IT will support IT-enabled investment programmes,[7] IT services and IT assets. IT should define how the objectives will be met, the measurements to be used and the procedures to obtain formal sign-off from the stakeholders. The IT strategic plan should cover investment/operational budget, funding sources, sourcing strategy, acquisition strategy, and legal and regulatory requirements. The strategic plan should be sufficiently detailed to allow for the definition of tactical IT plans.[8]

The OCFO should seek assistance from the Office of the Chief Technology Officer (OCTO) in developing its IT Strategic Plan pursuant to D.C. Code § 1-1403(8) (Supp. 2011), which states that one of OCTO's functions is to:

> Serve as a resource and provide advice to District departments and agencies about how to use information technology and telecommunications systems to improve services, including assistance to departments and agencies in developing information technology strategic plans[.]

OIG auditors also requested appropriate supporting documentation such as an applications inventory that would be helpful in creating an IT Strategic Plan and, in turn, strengthen the IT governance for the agency. We found that this documentation did not exist. TSG management created a listing of applications to assist with the audit. This listing was not comprehensive because it only included applications hosted by TSG, rather than applications critical to OTR's mission, and did not identify any information useful for strategic planning purposes.[9] The

[7] British English spelling.

[8] A tactical IT plan is a medium-term (i.e., 6- to 18-month range) plan that translates the IT strategic plan direction into required initiatives, resource requirements, and ways in which resources and benefits will be monitored and managed.

[9] Such strategic planning information would include: identification of process and application owners; key operation statistics; hardware; software; platform; source; version; availability of operating system, database and application support; date of last major upgrade; process owners; significance or ranking within OTR and its administrations; interfaces; degree of documentation; inclusion in disaster recovery plan; status (active, legacy, sunset); etc.

applications inventory should minimally identify mission-critical functions and the IT infrastructure used to support those functions. A current and comprehensive inventory of all applications greatly enhances an organization's ability to align its IT infrastructure more closely with its strategic objectives. Also, this management tool would assist various stakeholders, with different levels of IT knowledge, in obtaining an understanding of the current state of the IT infrastructure in order to facilitate the identification of future system requirements and needs.

In sum, the CIO, in conjunction with an IT strategy committee, has not developed and documented a clearly defined IT strategic plan. Further, OTR managers and stakeholders are not afforded a consolidated vehicle, such as a documented IT strategic plan, that articulates its IT vision, needs, goals, and objectives. Such a plan helps responsible IT managers understand and align their activities with the strategic direction of the agency's key business processes. An IT strategic plan will, in turn, enhance the effectiveness of IT governance by providing a good control mechanism that will enable responsible management personnel to consistently meet IT expectations, measure IT performance, manage related resources, and mitigate IT risks.

RECOMMENDATIONS, MANAGEMENT RESPONSES, AND OIG COMMENTS

We recommend that the Chief Information Officer, OCIO:

1. Develop and maintain an IT strategic plan aligned with OTR's strategic objectives.

OCIO RESPONSE

OCIO agreed with the recommendation and developed an IT strategic plan. This plan documents the alignment of the OCIO's goals and objectives with the OCFO's Guiding Principles, which include OTR's strategic objectives. This document will be reviewed and updated annually.

OIG COMMENT

Action taken by OCIO is responsive and meets the intent of the recommendation.

2. Continue to develop and implement an IT process framework that will accommodate the development and maintenance of an IT strategic plan.

OCIO RESPONSE

OCIO agreed with the recommendation and stated that there is currently a process in place to evaluate initiatives on a quarterly basis to make sure that projects are on track and aligned with the OCIO goals and objectives. The results of these quarterly evaluations are reviewed annually to update the strategic plan, ensuring that alignment with OCFO's business objectives is maintained.

FINDINGS AND RECOMMENDATIONS

OIG COMMENT

Action taken by OCIO is responsive and meets the intent of the recommendation.

3. Create a comprehensive applications inventory to assist various stakeholders in making and supporting strategic business decisions.

OCIO RESPONSE

OCIO agreed with the recommendation and currently maintains a comprehensive inventory of all the applications that they support for the OCFO's business units.

OIG COMMENT

Action taken by OCIO is responsive and meets the intent of the recommendation.

4. Adopt an established IT governance model, such as COBIT, to integrate and institutionalize good practices that ensure IT resources are appropriately used to support OTR's business objectives.

OCIO RESPONSE

OCIO agreed with the recommendation and stated that it established a Project Management Office (PMO) in 2009. The PMO's mission is to provide an enterprise-wide approach to the identification, prioritization, and successful execution of a portfolio of technology initiatives that are aligned with the strategic goals, business drivers and vision of the OCFO. The OCIO's IT governance framework is developed based on PMI [Project Management Institute] Methodology, Gartner Framework, and the processes and practices OCIO developed in house.

OIG COMMENT

Action taken by OCIO is responsive and meets the intent of the recommendation.

FINDINGS AND RECOMMENDATIONS

FINDING 2: APPLICATION SUPPORT

SYNOPSIS

OTR has not adequately addressed potential ITS application support risks associated with the use of COTS applications and custom modifications through its past and existing third-party contracts, which lack source code escrow[10] agreements and requirements to provide adequate and necessary system documentation in the event that a third-party contractor is unable or unwilling to maintain and update the application software. Additionally, OTR lacks system configuration documentation that affords OTR knowledge of the status of existing application controls used in revenue protection checks. We attribute these conditions to poor planning in the contracting, procurement, and system development processes.

As a result of the lack of escrow agreements and documentation requirements in COTS contracts, OTR had to evaluate the current state of the application and perform IT support through trial and error. Performing these processes through trial and error results in excessive time to develop mission critical changes, thereby increasing the risk of unforeseen errors when performing those changes, and potentially compromising existing application controls.

DISCUSSION

OTR did not obtain source code escrow agreements for TAS, CAMA, and IDCS, which are COTS software systems. Based on discussions with OCIO management, the reason the escrow agreements were omitted from the service contracts for these applications is unknown because OCIO procured these applications before the OCFO hired the current contracting officer. This may have occurred as a result of poor contract planning, excessive reliance on the contractor, and the lack of an IT control standard that requires third-party source code escrow agreements. Proper operation and maintenance of COTS software are critical to the continuing tax collection function at OTR. If the software manufacturer goes out-of-business, not having the source code available for modification could impact business operations by increasing the number and frequency of manual operations or result in other inefficient workarounds. This condition may have a significant impact on the cost to maintain current service levels to the District.

[10] Source code is the version of software as it was originally written in a human-readable programming language. Source code escrow is the deposit of the source code of software with a third party escrow agent. Escrow is typically requested by a party licensing software (the licensee), to ensure maintenance of the software. The software source code is released to the licensee if the licensor files for bankruptcy or otherwise fails to maintain and update the software as promised in the software license agreement.

This risk was realized when the contract between the TAS vendor, Accenture, and OTR was not renewed in February 2009. The source code escrow agreement for TAS did not exist and after several attempts, OTR was unable to obtain adequate system documentation and manuals for IT users to efficiently maintain the TAS application. The contracts for CAMA and IDCS pose a similar business risk because they also lack source code escrow agreements.

According to COBIT, the industry standards for managing third-party agreements and associated risks are described below:

> DS2 Manage Third-party Services
>
> The need to assure that services provided by third parties (suppliers, vendors and partners) meet business requirements requires an effective third-party management process. This process is accomplished by clearly defining the roles, responsibilities and expectations in third-party agreements as well as reviewing and monitoring such agreements for effectiveness and compliance. Effective management of third-party services minimises[11] the business risk associated with non-performing suppliers.
>
> DS2.3 Supplier Risk Management
>
> Identify and mitigate risks relating to suppliers' ability to continue effective service delivery in a secure and efficient manner on a continual basis. Ensure that contracts conform to universal business standards in accordance with legal and regulatory requirements. Risk management should further consider non-disclosure agreements (NDAs), escrow contracts, continued supplier viability, conformance with security requirements, alternative suppliers, penalties and rewards, etc.

OTR did not obtain critical system documentation and ensure adequate knowledge transfer from Accenture when the contract ended, which significantly impacted OTR and Revenue Solutions, Inc.'s (RSI) ability to efficiently and effectively support and maintain the TAS application. Unfortunately, without the critical system documentation from the vendor (e.g., data dictionary, data flow diagrams, system design documentation, business logic, etc.), all that remains is documentation within the source code, which is an inefficient and possibly ineffective[12] method to obtain information and evaluate risks associated with system modifications. TSG uses a change management tracking system to escalate and correct system issues, which, by design,

[11] British English spelling.

[12] The documentation may be ineffective in mitigating the risks of change because the purpose of inserting comments is to annotate the source code to make it easier for programmers to understand. The documentation also may not fully reflect interrelationships and data dependencies.

retains system alterations and can be used as reference documentation, but is not a substitute for complete and current system documentation.

Complete and current system documentation is required to maintain ITS applications. Industry standards and COBIT require that system documentation is maintained and updated to ensure effective utilization and maintenance of the system. OTR maintains that its current documentation process is adequate and that additional resources should not be spent on the current system, which is going to be replaced. OIG agrees that extensive documentation is unnecessary. However, fundamental and necessary system knowledge should be written and updated to support application maintenance in the event that the primary application developer becomes unavailable.

According to COBIT, the industry standard for acquiring and maintaining application software, including managing changes, is described below:

> AI4 Enable Operation and Use
>
> Knowledge about new systems is made available. This process requires the production of documentation and manuals for users and IT, and provides training to ensure the proper use and operation of applications and infrastructure.
>
> AI6.5 Change Closure and Documentation
>
> Whenever changes are implemented, update the associated system and user documentation and procedures accordingly.

Additional internal control deficiencies resulted from termination of the Accenture contract. Many of the TAS business application rules, or system configurations, that determine how a return is processed are embedded into the application code. OCIO advised that due to limited resources, a decision was made to omit the administrative screens within TAS for modifying business rule logic. Therefore, programmers are required to modify the business rules, which is one reason why OTR is replacing the current system. There is no system documentation to detail the mapping of business rules, their parameters, and the current state of the rules (i.e., active vs. inactive). Our audit found that there is currently no formal review process of the business rules to ensure that risks are properly mitigated; rules are currently applicable; controls are active or inactive; and rules comply with District laws and regulations.

According to COBIT, the industry standard for managing software configuration is described below:

> DS9 Manage the Configuration
>
> Ensuring the integrity of hardware and software configurations requires the establishment and maintenance of an accurate and complete configuration repository. This process includes collecting initial configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository as needed. Effective configuration management facilitates greater system availability, minimizes production issues and resolves issues more quickly.
>
> DS9.3 Configuration Integrity Review
>
> Periodically review the configuration data to verify and confirm the integrity of the current and historical configuration.

We believe that the absence of documented IT governance standards contributes to OTR's failure to adequately address potential business risks associated with the use of its COTS applications. Adequate application support documentation is necessary to mitigate risks associated with application maintenance in a manner that continues to provide for availability, confidentiality, and integrity of taxpayer data. The ability to administer and enforce the District's tax laws and collect revenue is dependent upon the information systems performing effectively without experiencing a critical failure or disruption.

RECOMMENDATIONS, MANAGEMENT RESPONSES, AND OIG COMMENTS

We recommend that the Chief Financial Officer, OCFO:

5. Require future COTS software acquisitions to include a source code escrow agreement in the vendor contract.

OCFO RESPONSE

OCFO agreed with the recommendation and stated that it will include a source code escrow agreement/clause in all future vendor contracts for COTS software acquisitions.

OIG COMMENT

Action taken by OCFO is responsive and meets the intent of the recommendation.

6. Require future third-party system vendors to create, update, and supply upon termination adequate system documentation for applications and modifications they support. When documentation is not obtained or available from third-parties, OCIO should create adequate

system documentation to support application maintenance. Additionally, when changes are performed by OCIO, the associated documentation should be updated as appropriate.

OCFO RESPONSE

OCFO agreed with the recommendation and stated that system design documentation is developed by both OCFO employees and the current TAS support vendor for modifications to the system. For future third-party systems the OCFO will require vendors to create, update and supply, upon termination, adequate system documentation.

OIG COMMENT

Action taken by OCFO is responsive and meets the intent of the recommendation.

7. Document the system configuration, including the status of critical application controls, and perform periodic reviews to determine whether configuration changes comply with business and regulatory requirements.

OCFO RESPONSE

OCFO agreed with the recommendation and stated that it has documented the business rules related to the critical application controls associated with TAS review items. This system documentation details the mapping of related business rules, their parameters and the current state of the rules (i.e., active versus inactive). A formal review of these business rules was initiated in October, 2012 to ensure risks are properly mitigated.

OIG COMMENT

Action taken by OCFO is responsive and meets the intent of the recommendation.

FINDINGS AND RECOMMENDATIONS

FINDING 3: APPLICATION CONTROLS

SYNOPSIS

Our audit found that OTR has application control deficiencies related to compliance with documented policies and procedures, penalty regulations, and best practices for fraud prevention. Specifically, we found that OTR does not: (1) enforce a provision of the District of Columbia Municipal Regulations (DCMR) requiring large filers to file and pay taxes electronically, and assess or collect the penalty for noncompliance; (2) reconcile withholding payments received to withholding amounts reported on individual tax returns; (3) utilize certain application controls to detect unapproved changes within the real property appraisal system; and (4) document taxpayer authorization for electronically filed (e-file) individual tax returns by OTR employees.

We attribute these control deficiencies to inadequate management oversight of documented policies and procedures and insufficient application controls. As a result, OTR failed to collect $6.5 million in penalty revenue and adequately minimize the risk of tax fraud and errors.

DISCUSSION

Application controls are automated controls within an IT system designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected. Application controls within ITS help ensure that transactions are authorized, valid, and accurately and completely processed. Both OTR and TSG are responsible for these application controls because the responsible business unit defines the requirements, while IT support translates those business requirements into system functionalities that process transactions accurately. During our review to determine whether ITS application controls – defined by laws and business requirements – are present, adequate, and functioning as intended, we found deficiencies in the following areas: (1) non-individual electronic file penalty; (2) reconciliation of withholding payments; (3) property valuation; and (4) unsigned individual tax returns.

Non-Individual Electronic File Penalty

Non-individual taxpayers (business entities) are required to file and pay taxes electronically if the amount of the payment exceeds $10,000.[13] This statutory requirement is codified at D.C.

[13] Prior to enactment of the Non-Individual Income Tax Electronic Filing Act of 2009 (Non-Individual e-File Act), D.C. Law 18-111, on March 3, 2010, the amount of the payment had to exceed $25,000 to require electronic payment. In addition, OTR issued Notice 2009-06, *Electronic Funds Transfer Payment Threshold Reduced*, dated September 15, 2009, which states that business tax payments must be filed electronically if the payment amount due for a particular period "is equal to or exceeds $10,000." *Available at*

Code § 47-4402(c), which specifies that the Mayor may require non-individual taxpayers to make payments electronically.

The Mayor requires electronic payments in accordance with the regulation entitled "General Requirements for Filing Tax Returns Including Electronic [Internet] Filing" (9 DCMR § 105), which sets forth rules to implement the provisions of the Non-Individual e-File Act. In addition, 9 DCMR § 105.13 sets forth a defined penalty for noncompliance equal to 10 percent of the amount due as shown on the tax return. Additionally, OTR administers the "Output Review Unit, Income & Business" (OCFO Financial Policies and Procedure Manual, Volume VIII, Section 35202003) policy, which states: "If [a] taxpayer(s) liability is more than $10,000.00 per period, taxpayer(s) must file and pay electronically...."

During our application control review, we noted that TAS is configured to automatically send notices to taxpayers for noncompliance with this requirement but the application did not contain a method for assessing or collecting the penalty for noncompliance. We found after further inquiry that OTR has neither assessed the penalty specified in the regulation nor enforced compliance with the criteria listed above. OTR failed to collect at least $6.5 million in penalty revenue as a result of not enforcing the 10 percent penalty for noncompliance according to 9 DCMR § 105.13. We calculated the amount of lost revenue based on the following:

- available data from March 16, 2006, to November 16, 2011;
- the number of notices OTR sent to non e-filers whose tax liability exceeded $10,000;[14]
- noncompliance more than 60 days after the first notice;
- minimum tax liability the penalty could be assessed upon; and
- the supposition that the taxpayer complied after the first penalty assessment.

Management maintains that the 10 percent penalty assessment is not enforceable because of the ambiguity and lack of a defined penalty within the law. However, between March 16, 2006, and November 16, 2011, OTR mailed a total of 31,444 formal notification letters to noncompliant taxpayers with instructions on how to electronically file in order to become compliant.

Reconciliation of Withholding Payments

OTR does not match withholding payments received from employers to the tax payments reported on individual tax returns. Withholdings are income taxes withheld from taxpayers'

http://otr.cfo.dc.gov/otr/cwp/view,a,1328,q,593561.asp (last visited Nov. 5, 2012). (Follow the "Notices" hyperlink under "Reference Materials.").

[14] *Id.*

wages and paid directly to the District by the taxpayers' employers. If the amounts are not reconciled, there is a risk that tax refunds may be issued in error without verifying that the taxpayers had withholding payments made on their behalf.

OTR managers indicated that a preventive control is not feasible because it would hinder the timely processing of refunds due to many employers filing paper returns. Prior to the 2012 tax filing season, District law did not contain an adequate timely employer W-2 filing requirement, pursuant to D.C. Code § 47-1812.08 (Withholding of Tax), for OTR to perform a preventive control to prevent improper refunds from occurring. The paper-based employer W-2 annual filings need to be received timely by OTR and then converted to an electronic format for comparison. Therefore, management indicated that reconciling withholding information is not feasible during tax filing season. In time for the 2012 tax filing season, temporary D.C. Law 19-0090[15] was enacted to promote timely W-2 filing by January 31, 2012. D.C. Law 19-0090 also requires employers filing more than 25 W-2 statements to e-file. While the number of employers that e-file is increasing, there is currently no penalty prescribed in the D.C. Code, D.C. Law 19-0090, or in any regulation for noncompliance or late filing. Therefore, it is unclear how well the W-2 e-filing requirements can be enforced.

Additionally, OTR did not have a detective control in place at the time of our audit. However, OTR did perform a pilot matching or reconciliation procedure using electronic tax filings from TY 2008, in response to a similar finding cited by BDO Seidman, LLP.[16] OTR informed OIG auditors that this process was discontinued due to a combination of factors, including employee turnover, lack of resources, inadequate statutory employer withholding filing requirements, and the number of paper-based employer withholding returns.

OIG auditors performed a limited review based on the available data and documentation regarding this pilot procedure provided by the Compliance Administration within OTR. Our review identified errors in the pilot reconciliation procedure where incorrect withholding amounts were attributed to the wrong taxpayer. In some cases, this problem occurred with relationships between profiles, such as when the withholding amounts were reversed for a husband and wife.

OTR management stated that only nominal benefits were realized and, therefore, did not pursue this program in subsequent tax years. However, this type of control is currently used by other states, and we strongly believe its use will enhance data integrity and fraud detection for the District government.

Management Corrective Action: Even though the initial W-2 verification program was discontinued, OTR management is currently seeking this functionality in the future replacement

[15] D.C. Law 19-0090 modified D.C. Code § 47-1812.08 (Withholding of Tax), and expired on October 6, 2012.
[16] External CAFR auditor responsible for the "District of Columbia Independent Auditors' Report on Internal Control Over Financial Reporting and on Compliance and Other Matters Based on an Audit of Financial Statements Fiscal Year Ended September 30, 2008."

tax administration system, the Modernized Integrated Tax System (MITS). The Request for Proposal[17] requires the MITS to be capable of "Verifying W-2 data claimed on the return by comparing to employer-submitted W-2 data." Moreover, management maintains that, due to the change in employer filing requirements and increased electronic conversion efforts within OTR, a post-audit verification program will be in place for the 2012 tax filing season.

Property Valuation

The OIG auditors sampled 2,524 properties in CAMA and identified 26 with unapproved characteristic[18] changes that occurred during the Annual Valuation and Review Process ("Review Process"), which occurs between October 1st and the first week in February for District real property. During this period, assessor changes to property characteristics can be made without a supervisor's knowledge and approval.

Out of 143 residential neighborhoods, we randomly selected 3 neighborhoods from the 2013 approved "Percentage Change Detail Analysis" completed work file. The sample we selected for testing included property characteristic changes tracked in CAMA (audit trail), occurring between December 2011 and February 2012, which affected property valuations and ultimately the amount of property tax assessed. We compared the value in the CAMA system to the value that was manually approved on the "Percentage Change Detail Analysis" report by the supervisor. The changes we identified occurred after the printing of the report and demonstrated that modifications to property records were occurring without being visible to management. OTR management reviewed our exceptions and concluded that none of the adjustments in the sample were fraudulent or erroneous, and that they were ordinary and necessary changes. We do not dispute this assessment.

However, the current method of review, using printed reports by neighborhood, does not allow for visibility of changes during the review process. Also, the prior year's unapproved values will be shown in the subsequent year's review, which may continue to hinder detection of inappropriate changes. This problem occurs because the process generates reports at a specific point in time for review while the assessors make changes to property record cards on a continual basis. Additionally, according to OTR management, the values change due to final calibration of the property valuation model, which is an iterative and collaborative process used to validate subsequent TY property valuations.

Therefore, the current process may fail to detect inadvertent errors or fraud during OTR's review process. OTR management maintains the process is adequate due to a compensating manual control, which includes a high-level review of old to new valuations that should identify substantial changes requiring further examination. However, we regard proper review, approval,

[17] Solicitation Number CFOPO-12-R-004, Modernized Integrated Tax System (Feb. 20, 2012).

[18] Property "characteristics" include information specific to individual properties such as: type of construction, square footage, and condition. This information is maintained on the electronic property record card within the CAMA database.

and visibility of changes in property characteristics to be necessary key controls to reduce the potential occurrence of errors and fraud.

Unsigned Individual Tax Returns

During process walkthroughs and discussions with management, we noted that Customer Service Administration (CSA) employees in the OTR walk-in center were authorized to submit individual tax returns on behalf of taxpayers. This is a service OTR provides to District residents to assist them in filing their individual tax returns electronically. The control deficiency within this process indicates there is no record or documentation that the taxpayers authorized OTR employees to submit the returns on their behalf.

General Requirements for Filing Tax Returns Including Electronic [Internet] Filing (9 DCMR § 105.2) states:

> Each return filed shall be signed by the taxpayer, either under oath or otherwise, as the Deputy Chief Financial Officer shall prescribe in the form of return.

At the bottom of the D-40 Individual Income Tax Return form, the taxpayer's name is automatically populated in the signature line, which states, "Under penalties of law, I declare that I have examined this return and, to the best of my knowledge, it is correct." However, the OTR employee is the party authenticated through the eTSC log in screen and submitting the return, not the taxpayer. The eTSC system has an effective audit trail, which records a transaction number and the ID of the OTR employee submitting the return.

Additionally, there is no indirect evidence that the taxpayer filed the return. The queuing process OTR uses at the walk-in customer service center is anonymous. Thus, there is no record of the taxpayer visiting OTR on the date the return is filed. Also, the employees do not add a note to the taxpayer's account in the ITS because management does not require notes for this kind of transaction. Moreover, the taxpayer does not sign a hard copy of the tax return. As a result, there is no record that the taxpayers requested OTR employees to file returns electronically on their behalf. OTR assumes the risk that the taxpayers may deny the accuracy of these returns or that they did not authorize filing the returns. The risk is compounded where a taxpayer provides fraudulent information or falsified documents.

The Internal Revenue Service uses Form 8879, "IRS e-file Signature Authorization," which the taxpayer signs authorizing an agent to submit an electronic tax return on his or her behalf. This form supports and documents that the taxpayer reviewed key amounts reported and authorized the tax return filing. OTR could implement a similar form because it is capable of creating and imaging such a document utilizing existing information system resources.

Overall, these application control deficiencies increase the risk that compliance failures, errors, fraud, and other improprieties within the District's tax administration processes may not be prevented or detected timely.

RECOMMENDATIONS, MANAGEMENT RESPONSES, AND OIG COMMENTS

We recommend that the Chief Financial Officer, OCFO:

8. Request that the Office of the Attorney General (OAG) opine on the enforceability of the penalty set forth in 9 DCMR § 105.13, which is an implementing regulation for the Non-Individual e-File Act. Dependent upon OAG's response, OTR should enforce the regulation or request that the Council of the District of Columbia amend D.C. Code § 47-4402(c) to allow for effective enforcement of the 10 percent penalty for noncompliance.

OCFO RESPONSE

OCFO agreed with the recommendation and stated that it referred this matter to the OCFO General Counsel for advice. OTR will be guided by their response.

OIG COMMENT

Action planned by OCFO is responsive and meets the intent of the recommendation. However, OCFO did not provide an estimated target date for the completion of planned actions for this recommendation. Thus, we respectfully request that OCFO provide a target date for planned corrective action within 60 days of the date of this final report.

9. Develop and implement a preventive or detective control process to regularly reconcile withholding payments received from employers to the withholding amounts indicated on the tax returns.

OCFO RESPONSE

OCFO disagreed with the recommendation then stated that a post-filing [detective control] audit program would be pursued when the necessary automation was in place. Due to resource constraints, no programming was completed on this project in FY 2012. However, OTR continues to recognize the risks associated with potential W-2 fraud, and has in place compensating controls that provide significant mitigation for the risk of issuing fraudulent refunds. With mitigating [preventative] controls in place, OTR continues to believe this [detective control] to be a lower priority compliance project. Additionally, real time data matching [overall preventative control] cannot be accomplished because of the variance between the time that taxpayers begin filing and the date when employer withholding must be reported, even under the accelerated deadline.

OIG COMMENT

OCFO's response is noted, but does not explicitly meet the intent of this recommendation. The detective control proposed may accurately establish the extent of fraud occurring; prioritize enforcement actions; facilitate the development of processes, procedures and legislation necessary to develop an overall preventative control; and contribute to the cost benefit analysis needed to justify the inclusion of such a control when the current TAS application is replaced. While OTR did not concur with the recommendation based on mitigating preventative controls being utilized, it also stated that the proposed detective control would be implemented when necessary automation is in place. Therefore, it is unclear to the OIG with which part of the recommendation that OCFO does not concur. As such, we respectfully request that OCFO provide a target date for planned corrective action or additional clarification on the points of disagreement within 60 days of the date of this final report.

10. Review D.C. Code § 47-1812.08 (Withholding of Tax) and determine whether an amendment to the law or a new regulation, to include a penalty, would promote compliance and enforceability.

OCFO RESPONSE

OCFO agreed with the recommendation and will undertake a study to determine whether the application of a penalty charge is necessary to promote compliance with the requirement for employers to file W-2 statements electronically.

OIG COMMENT

Action planned by OCFO is responsive and meets the intent of the recommendation. However, OCFO did not provide an estimated target date for the completion of planned actions for this recommendation. Thus, we respectfully request that OCFO provide a target date for planned corrective action within 60 days of the date of this final report.

11. Revise the current annual valuation review process to ensure property characteristic changes that affect assessed values in the CAMA system are reviewed and approved.

OCFO RESPONSE

OCFO disagreed with the recommendation and contends that the process, which includes a high-level mitigating control to be adequate in mitigating the risk of errors and fraud, and OTR considers the risk to be low.

FINDINGS AND RECOMMENDATIONS

OIG COMMENT

OCFO's response is noted, but does not meet the intent of this recommendation, which states that changes did and can continue to occur to property characteristics without management oversight during the annual valuation review process. These changes could affect the amount of tax collected on individual properties which may go undetected with a high level mitigating control. Accordingly, we respectfully request that OCFO reconsider its response to this recommendation and provide the OIG with a revised response within 60 days of the date of this report.

12. Require taxpayers to sign a form authorizing CSA personnel to complete an eTSC tax filing on their behalf and confirming that key line items from the return are accurate.

OCFO RESPONSE

OCFO made a business decision, unrelated to this finding, to disable eTSC for online individual tax filing due to the cost of maintenance and a wide variety of tax preparation software (including many who participate in the FreeFile Alliance). Because OTR is no longer using eTSC to prepare and file individual income tax returns on behalf of taxpayers, no actions will be taken to implement this recommendation. Additionally, the new process which CSA uses to assist taxpayers in filing returns recognizes and mitigates the risks associated with filing inaccurate or unauthorized returns.

OIG COMMENT

Action taken by OCFO is responsive and meets the intent of the recommendation.

FINDINGS AND RECOMMENDATIONS

FINDING 4: GENERAL CONTROLS

SYNOPSIS

Our audit found that there are weaknesses in the general controls[19] related to certain IT services performed by TSG in conjunction with certain business processes managed by OTR. Specifically, we noted that OCIO and OTR failed to effectively restrict access to TAS and CAMA applications according to job responsibilities or segregation of duties (SOD) considerations and implement application and general controls to safeguard the use of high-risk spreadsheets. Additionally, OCIO failed to: (1) implement an effective mechanism to deactivate user access in eTSC based on changes to business relationships in TAS; (2) afford the taxpayer an automated method for monitoring eTSC business account access; (3) implement a process to disable inactive user accounts in eTSC; and (4) restrict access to the eTSC production environment according to accepted SOD considerations for developers or, alternatively, implement compensating monitoring controls.

These conditions occurred due to insufficient management oversight and controls over access to applications. As a result, access to critical data and programs was not properly restricted. In addition, these control deficiencies increase the risk of unauthorized changes to data and programs that can adversely affect the confidentiality, integrity, and availability of computer-based data for compliance monitoring and decision-making purposes. The reliable and consistent operation of general controls within a time period is necessary to place reliance on application controls within the same period.

DISCUSSION

TSG maintains the IT infrastructure and performs IT-related service activities for many automated business processes at OTR. The IT general controls provide the foundation for a well-controlled technology environment in which computer-based application systems are developed, maintained, and operated. Such controls are essential to all applications at OTR.

Our audit included testing selected general controls that ensure: (1) proper development and implementation of applications; (2) integrity of programs, data files, and computer operations; and (3) compliance with recommended SOD requirements. Weaknesses in the design or execution of general controls can reduce the effectiveness of application controls through circumvention (e.g., direct data manipulation bypassing the application controls) or modification (e.g., unauthorized changes to an application's configuration). Our assessment of the ITS general controls noted deficiencies in the following areas: (1) user roles in TAS and CAMA; (2)

[19] IT “general controls” are the controls applied to all IT service activities. The reliable operation of these general controls is necessary for reliance to be placed on application controls and support the consistent processing and reporting of operational and financial data in accordance with applicable laws, regulations, and management directives. Some examples include: logical access, change management, and systems development.

spreadsheet controls; (3) eTSC logical access controls; (4) dormant user accounts; and (5) developers' access to the production environment.

User Roles in TAS and CAMA

Existing user-access controls to help prevent a single individual from performing incompatible functions or inappropriately accessing information are ineffective. Specifically, we identified: (1) conflicting roles that allow supervisors to perform the same tasks as their subordinates in TAS and CAMA with capabilities to circumvent proper review and approval; (2) conflicting responsibilities within roles or between multiple roles assigned to a single user allowing the user to initiate a transaction and edit demographic information[20] in TAS; and (3) TAS Application Security Administrators (ASA)[21] with the capability to alter their own access privileges to view employee and VIP[22] taxpayer information, thereby allowing inappropriate access to sensitive information.

Confidentiality and integrity of data are dependent on effective SOD controls. SOD is the practice of dividing incompatible functions in critical processes among different individuals to prevent one individual from having complete control over input, processing, and output of computer-processed data. Organizations typically take steps to ensure that they:

- Segregate incompatible duties and establish related policies to monitor incompatible functions based on risks;
- Establish access controls to enforce SOD requirements within the computer processing environment; and
- Restrict individuals from initiating and approving transactions through formal operating procedures, ongoing supervision, and regular reviews.

Computer access controls should limit users to those functions necessary to perform their jobs. Additionally, job responsibilities should not entail performing incompatible functions without adequate compensating controls. In implementing well-designed access controls, risk is reduced by removing unnecessary permissions, which could: (1) introduce unintentional errors; (2) facilitate fraudulent actions by users; and (3) allow unauthorized users to impersonate authorized users through theft of passwords.[23]

[20] Demographic information includes bank account numbers and taxpayer addresses. These incompatible functions could allow a user to create and misdirect a taxpayer refund.
[21] ASA is the position within each OTR Administration that administers access controls in the ITS for its staff.
[22] VIP taxpayer accounts are restricted from view and access for a specific reason (i.e., high profile person).
[23] There are various methods in which passwords could be compromised. However, they are often compromised by employees not following procedures to safeguard their passwords (e.g., writing a password on a post-it note).

FINDINGS AND RECOMMENDATIONS

COBIT PO4.11 Segregation of Duties standards require:

> Implement[ation of] a division of roles and responsibilities that reduces the possibility for a single individual to compromise a critical process. [Also, ensure] that personnel are performing only authorised[[24]] duties relevant to their respective jobs and positions.

OCTO Policy OCTO0003, Information Security Program, states:

> Employees and contractors will be granted only the level of access to information and automated systems they need to do their jobs. Additional access to sensitive information and systems shall not be provided until such access is needed and is formally authorized in accordance with District of Columbia government standards.

Approximately 45 percent of the user roles defined in TAS were authorized to perform two or more conflicting functions, thereby causing a SOD issue; such as allowing one user to make adjustments, approve refunds, and alter taxpayer bank account information. OTR Management indicated that this condition was caused by an inadequate redesign of user roles during CY 2008. Per management, this project failed because the various OTR Administrations[25] had more input than they should have had throughout this process. The employees within the Administrations did not want their roles restricted because they were accustomed to performing certain actions, and resisted Accenture's recommended role modifications. The end result was that newly defined user roles still had SOD issues and many users had more access than was necessary or prudent.

We discussed an additional SOD conflict with OTR management, which was that an ASA can maintain his or her own access to VIP and employee accounts. By changing this access, the ASA, who was formerly restricted from an account, is now able to view and perform edits in line with his or her existing role permissions. Management advised that this is a system design limitation and there is an existing mitigating control that reviews users, including ASAs, with VIP and employee access, on a quarterly basis.

CAMA supervisors possess authority to change property record cards, which contain the property characteristics affecting the valuation of individual properties. OTR management stated that while it is best for the appraiser to make these changes, it is not always practical or efficient in all situations and, therefore, supervisors must have the ability to make appropriate changes. To maintain appropriate SOD, supervisor access should be limited to review and approval of changes affecting property values.

[24] British English spelling.

[25] The OTR Administrations include the Compliance, Customer Service, Returns Processing, Revenue Accounting, and Real Property Administrations. (See Page 2, Figure 1.)

Management Corrective Action: OTR management shared with OIG auditors the preliminary documents reflecting newly developed TAS roles to correct SOD weaknesses in logical access. Prior to this audit, management also implemented manual mitigating controls to reduce the risk associated with the identified SOD weaknesses. These OTR actions should minimize the risk of errors and undetected fraud.

Spreadsheet Controls

The OIG auditors found that OTR lacked adequate general controls to protect spreadsheets that are used to perform critical tax assessment processes. Similar to other information systems, a spreadsheet should utilize built-in general and application controls based on risk. COBIT states that applications should be categorized by risk and protected accordingly to include a security plan, change management procedures, and business continuity plans.[26]

The low-level security inherent in the default settings within spreadsheets allows errors and fraud to go undetected and unchecked. We found the following controls were not applied in a spreadsheet used to calculate, manage, and record major commercial property valuations:

1. version control;
2. audit trail;
3. documented testing and authorization;
4. automated edit checks/data validation; and
5. documented policies and procedures addressing spreadsheet controls.

The risk of improperly altered formulas and data grows as the complexity and size of the spreadsheet increases. There were approximately 1,500 different formulas contained in this single spreadsheet. OTR management indicated that they had not considered applying general and application controls to its key spreadsheets. OIG auditors believe critical spreadsheets developed to handle key tax assessment processes and financial reporting should be classified by risk, and IT general controls should be applied to ensure confidentiality, integrity, and availability of data.

eTSC Logical Access Controls

Deactivated Business Accounts. Since eTSC's inception in CY 2001, the deactivation of accounts or user IDs in TAS has not carried forward to eTSC. OIG auditors identified 1,572 eTSC business accounts that were deactivated in TAS, but still active in eTSC. When an eTSC user ID related to a business account is deactivated in TAS during the nightly batch, the relationship should also be removed from the eTSC application in order to remove that user's logical access rights to the business' eTSC account. OTR management cited improper integration testing as the reason for this general control failure. However, this process has never

[26] COBIT DS5.2 IT Security Plan; AI6.1 Change Standards and Procedures; and DS4.2 IT Continuity Plans.

worked since eTSC's inception, which also confirms that this functionality has never been tested or reviewed.

Management Corrective Action: During the course of our audit, OTR management took corrective action regarding the deactivation functionality between TAS and eTSC applications. OIG auditors received documentation that TSG effectively restored and tested this deactivation functionality preventing unauthorized access to business tax accounts through eTSC.

Dormant User Accounts. The eTSC does not have an automated process in place to disable user accounts after extended periods of inactivity. We reviewed user account management for eTSC and identified many user IDs that have not been used for several years (See Table 1 below.) OIG auditors found that 41 percent of all eTSC user accounts have not been used in the last 3 years. Since the statute of limitations on filing is three years, we believe that most of the 31,063 IDs no longer require access to the corresponding tax accounts; however, the accounts are still active.

Table 1. Dormant eTSC User Accounts

Last Used More Than	Number of Unused IDs	Percentage Unused
5 years ago	19,330	25
3 years ago	31,063	41
2 years ago	37,913	49

Additional issues we identified with the user account management procedures include the following:

1. taxpayers are not afforded an automated method to monitor their account access;
2. taxpayers must contact OTR in order to deactivate their user IDs;
3. accounts must be manually deactivated regardless of extended periods of inactivity; and
4. the automated deactivation function from TAS to eTSC was not functioning prior to this audit.

We believe that inactive eTSC accounts should automatically expire after a set period of inactivity. Weak controls over user accounts allow unauthorized individuals to gain access to these accounts, which could lead to unauthorized disclosure of taxpayer data and potential fraudulent tax returns. Due to limited eTSC support, the MITS project, and the prioritization of several other pressing security and filing season readiness issues, OTR did not address the conditions related to inactive accounts.

Developers' Access to the Production Software Environment

OIG auditors found that two eTSC software developers had update access to the production software environment, which is an SOD conflict. Specifically, the developers had unlimited access to both the business and individual account software modules. This access could permit the developers to move unapproved or untested computer programming code to the production software environment. In order to maintain control over the production code,[27] it is necessary to provide assurance that the code is not being changed in an uncontrolled fashion. For instance, restricting access to read-only allows developers to see the code running in production and perform file comparisons that can be useful in troubleshooting, while reducing the risk of unauthorized code being introduced into the production environment.

OTR management explained that the developers were assigned access to the production software environment because the original contractor, responsible for code migration, at some point became inaccessible. Currently, OTR has a migration group responsible for this function so that no one person can circumvent the change management process. However, TSG could not explain the continued need for the developers' access to the production software environment.

Management Corrective Action: In response to OIG inquiries, TSG restricted the developers' access to read-only in the eTSC production software environment. This action adequately addressed the SOD issue noted by the OIG auditors.

The general control deficiencies in TAS, CAMA, eTSC, and critical spreadsheets increase the risk of unauthorized changes to critical tax administration data and programs. These conditions adversely affect the confidentiality, integrity, and availability of computer-based District tax data. Additionally, the logical access control deficiencies in eTSC allow unnecessary and unauthorized access to individual and business tax records. In order to minimize these risks, OCFO should evaluate the unaddressed control deficiencies noted in this section, and determine the best course of action to implement cost-effective solutions in the existing IT environment until the new system is implemented.

RECOMMENDATIONS, MANAGEMENT RESPONSES, AND OIG COMMENTS

We recommend that the Chief Financial Officer, OCFO:

13. Complete a comprehensive review and analysis of current user roles in TAS and CAMA to identify and correct segregation of duties control deficiencies.

OCFO RESPONSE

OCFO agreed with the recommendation and completed a comprehensive analysis and review (in April 2012) of current user roles in TAS, which included an individual assessment of the privileges granted to each of the OTR administrations to identify incompatible roles and

[27] The production code is the tested and approved version of the software used in the production (transaction processing) environment.

opportunities to improve segregation of duties [conflicts]. To correct segregation of duties control deficiencies within CAMA, an upgrade of the system is required (planned for FY 2013).

OIG COMMENT

Action taken and planned by OCFO is responsive and meets the intent of the recommendation. However, OCFO did not provide an estimated target date for the completion of planned actions related to the CAMA portion of this recommendation. Thus, we respectfully request that OCFO provide a target date for planned corrective action within 60 days of the date of this final report.

14. Identify and classify the agency's use of spreadsheets based on risk and indicate their importance in the proper functioning of key controls in the tax administration process.

OCFO RESPONSE

OCFO response has been redacted at its request.

OIG COMMENT

OCFO's redacted response has been noted, but it did not meet the intent of this recommendation, which is to identify additional high risk spreadsheets used by OTR in tax collection and financial reporting processes. Accordingly, we respectfully request that OCFO reconsider its response to this recommendation and provide the OIG with a revised response.

15. Implement IT general and application controls to ensure the confidentiality and integrity of data and calculations within all high-risk spreadsheets.

OCFO RESPONSE

OCFO partly agreed with the recommendation and stated that controls will be implemented on the spreadsheets used for valuation, until their use is discontinued with the implementation of a new CAMA system by the end of [CY] 2013.

OIG COMMENT

OCFO's response is noted, but does not meet the intent of this recommendation, which is to implement controls on all high-risk spreadsheets identified in Recommendation 14. Accordingly, we respectfully request that OCFO reconsider its response to this recommendation and provide the OIG with a revised response.

16. Develop and implement an automated method for taxpayers to manage and/or monitor eTSC business account access.

OCFO RESPONSE

OCFO agreed with the recommendation and deferred implementation because of the planned system replacement project, which includes eTSC functionality. The replacement project includes requirements for taxpayer management and monitoring of business accounts within a Taxpayer Web Portal.

OIG COMMENT

Action planned by OCFO is responsive and meets the intent of the recommendation. However, OCFO did not provide an estimated target date for the completion of planned actions for this recommendation. Thus, we respectfully request that OCFO provide a target date for planned corrective action within 60 days of the date of this final report.

17. Create, test, and implement an application control for eTSC to disable user accounts after a set period of inactivity.

OCFO RESPONSE

OCFO disagreed with the recommendation and stated that disabling eTSC user accounts after a set period of inactivity would cause an unnecessary burden on taxpayers that use the application annually.

OIG COMMENT

OCFO's response is noted, but does not meet the intent of this recommendation. We noted that 41 percent of the eTSC user accounts have not been used in the last 3 years, which may increase the likelihood of inappropriate access to these accounts and unauthorized disclosure of taxpayer data. While disabling user accounts after 90 or 180 days of inactivity may be burdensome to taxpayers as described in the OCFO response, a longer interval not to exceed 3 years should be considered. Accordingly, we respectfully request that OCFO reconsider its response to this recommendation and provide the OIG with a revised response within 60 days of the date of this final report.

18. Ensure continuous compliance with the proper segregation of duties standard by maintaining the developers' read-only access to the production software environment.

OCFO RESPONSE

OCFO agreed with the recommendation and stated it will ensure continuous compliance with the proper segregation of duties standard by maintaining read-only access to the production environment.

OIG COMMENT

Action taken by OCFO is responsive and meets the intent of the recommendation.

OTHER MATTERS OF INTEREST

Our audit identified the following issues indirectly related to the ITS application control review during process walkthroughs and other testing: (1) duplicate refund; (2) missing restrictive endorsement; (3) misuse of manual penalty; and (4) correspondence resolution tracking. Even though these manual control deficiencies fell outside the scope of the audit, we believe the potential risk for fraud, inefficiency, and errors warranted OTR management's attention. We investigated these deficiencies, discussed remediation strategies, and followed up to ensure proper escalation and resolution where management agreed that the risk was significant. Descriptions of the issues and OTR management corrective actions are detailed below.

DUPLICATE REFUND

OIG auditors alerted OTR management to a duplicate refund occurrence, which resulted from filing the same tax return on two different tax form types for the same tax year. This was an inadvertent taxpayer error. While the application controls built into the system suspended the second return, there were failed manual controls that circumvented the system and resulted in OTR issuing a duplicate refund to the taxpayer. OTR management took immediate corrective action and was attempting to recover the funds.

MISSING RESTRICTIVE ENDORSEMENT

OTR receives, records, and remotely and manually deposits tax payment checks. Currently, these checks are not restrictively endorsed, which would minimize the potential for check fraud. The risks associated with the lack of a restrictive endorsement include duplicate presentment, safekeeping, destruction, and retrieval. While OTR has not experienced this type of fraud, it occurred in another D.C. OCFO department 2 years ago. OTR management maintains that the restrictive endorsement process is becoming obsolete due to Check 21[28] and remote data capture of electronic bank deposits.

MISUSE OF MANUAL PENALTY

During a compliance test of penalties and interest, we found that a manual tax penalty adjustment was used to process aged franchise short-year returns as a workaround within the ITS. After further probing, the underlying issues were that users did not know how to use the system to process short-year returns as intended, policies and procedures inadequately described how to perform this process, and the issue was never formally communicated to operations management or TSG for problem resolution. Once the OIG informed operations management and TSG, they took immediate corrective action by testing the system for functionality, rewriting the procedures for this task, and training staff on the proper use of ITS to process this type of return.

[28] The Check Clearing for the 21st Century Act, or the Check 21 Act, Pub. L. No. 108-100, 117 Stat. 1177, is a federal law that took effect on October 28, 2004, and gives banks and their organizations the ability to create electronic image copies of consumers' checks. This law aims to make use of technology to reduce or eliminate the costs involved with paper check processing.

OTHER MATTERS OF INTEREST

CORRESPONDENCE RESOLUTION TRACKING

OTR is not tracking taxpayer correspondence through to the end of the resolution process, thereby resulting in untimely responses from the Customer Service Administration (CSA) or, in some instances, no response at all. OIG auditors alerted CSA management to a 10-month old unanswered taxpayer letter requesting abatement of penalties and interest that we observed during a walkthrough. The system tracking ended when the status was set to "Closed" by a CSA employee in the Seibel Correspondence Tracking System (CTS). The CSA employee subsequently noted the taxpayer account in ITS and manually handed the approval request to his supervisor according to OTR procedure. However, the supervisor did not complete the manual procedures to review the request, note the determination in the ITS account, and mail a resolution to the taxpayer. OTR paid additional interest to this taxpayer because of the delayed response.

The supervisor explained that the failure in this process occurred due to time constraints, other priorities, and high turnover in CY 2010. We observed that written correspondence was the lowest priority, while in-person taxpayer requests, and those that were emailed and phoned were handled first. OIG auditors recommended that the status of correspondence should only be set to "Closed" in CTS upon final resolution. The Acting CSA Director agreed with this recommendation.

EXHIBIT A: SUMMARY OF POTENTIAL BENEFITS RESULTING FROM AUDIT

Recommendations				
No.	**Description of Benefit**	**Amount and Type of Benefit**	**Estimated Completion Date**	**Status**[29]
1	**Internal Control, Economy and Efficiency.** Ensures alignment of IT expenditures with business strategies.	Non-Monetary	4/5/2013	Closed
2	**Internal Control, Economy and Efficiency.** Ensures policies are in place to facilitate the development and maintenance of an IT strategic plan.	Non-Monetary	4/5/2013	Closed
3	**Internal Control, Economy and Efficiency.** Facilitates the organization's ability to align its IT infrastructure more closely with its strategic objectives.	Non-Monetary	4/5/2013	Closed
4	**Internal Control.** Ensures good IT practices are institutionalized to support business objectives.	Non-Monetary	4/5/2013	Closed
5	**Internal Control.** Minimizes risk associated with the use of COTS software.	Non-Monetary	4/5/2013	Closed
6	**Economy and Efficiency.** Requires adequate system documentation to effectively support and maintain applications.	Non-Monetary	4/5/2013	Closed
7	**Compliance and Internal Control.** Ensures accuracy of system configuration and compliance with business and regulatory requirements.	Non-Monetary	10/31/2012	Closed

[29] This column provides the status of a recommendation as of the report date. For final reports, **"Open"** means management and the OIG are in agreement on the action to be taken, but action is not complete. **"Closed"** means management has advised that the action necessary to correct the condition is complete. If a completion date was not provided, the date of management's response is used. **"Unresolved"** means that management has neither agreed to take the recommended action nor proposed satisfactory alternative actions to correct the condition.

EXHIBIT A: SUMMARY OF POTENTIAL BENEFITS RESULTING FROM AUDIT

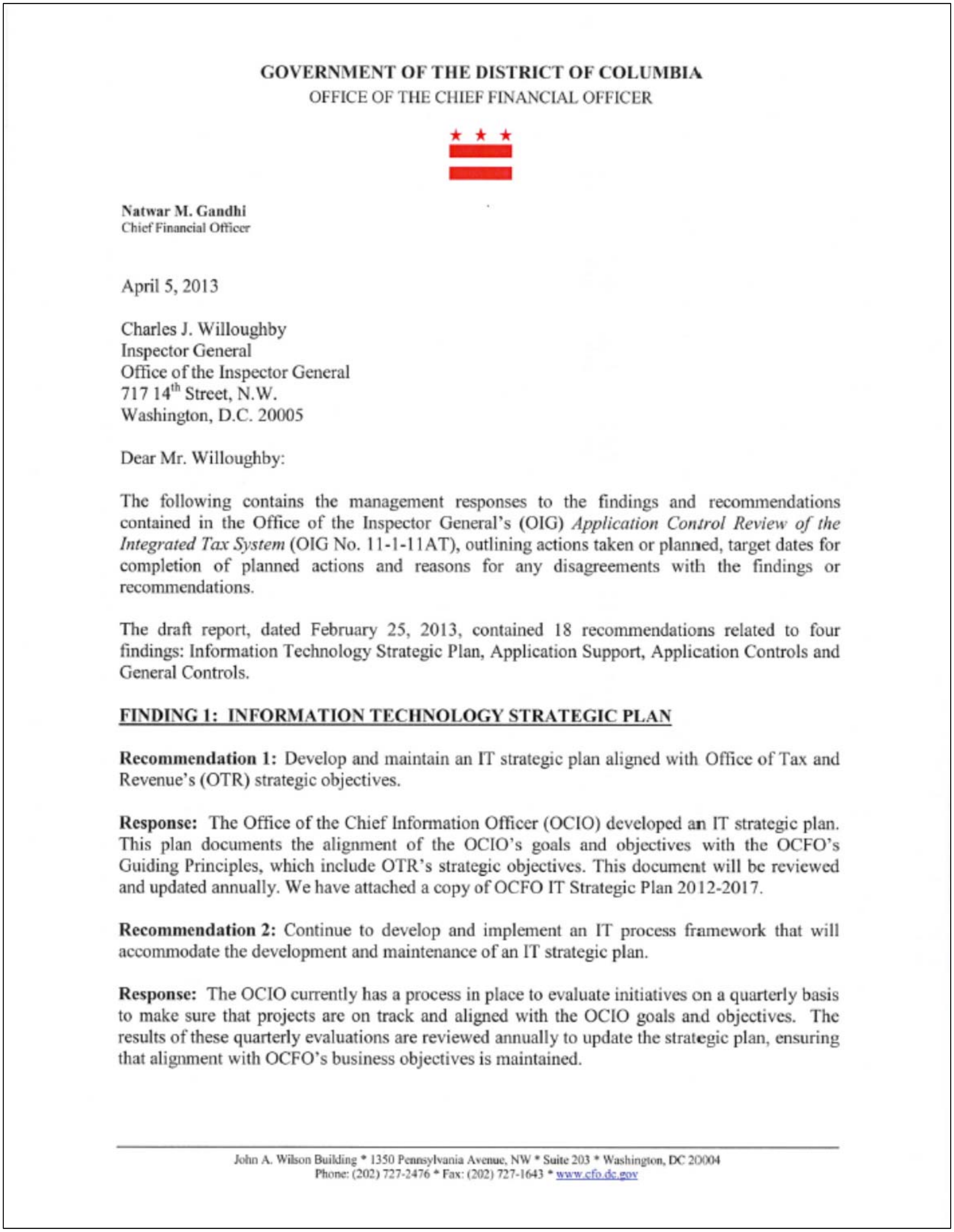
Recommendations (continued)

No.	Description of Benefit	Amount and Type of Benefit	Estimated Completion Date	Status
8	**Compliance.** Determines enforceability of the penalty provision of the Non-Individual e-File Act implementing regulations and potential collection of penalty revenue.	Monetary $6.5 Million	TBD	Open
9	**Internal Control, Economy and Efficiency.** Reduces the risk of issuing erroneous or fraudulent refunds.	Non-Monetary	TBD	Unresolved
10	**Compliance and Internal Control.** Facilitates effective compliance and enforceability of withholding reporting requirements.	Non-Monetary	TBD	Open
11	**Internal Control.** Minimizes the risk of errors and fraud affecting real property valuations during the annual valuation process.	Non-Monetary	TBD	Unresolved
12	**Compliance and Internal Control.** Effectively assigns e-filing responsibility to the taxpayer.	Non-Monetary	4/5/2013	Closed
13	**Internal Control.** Minimizes the risk of errors and fraud associated with users being able to perform incompatible functions.	Non-Monetary	TBD	Open

EXHIBIT A: SUMMARY OF POTENTIAL BENEFITS RESULTING FROM AUDIT

Recommendations (continued)				
No.	**Description of Benefit**	**Amount and Type of Benefit**	**Estimated Completion Date**	**Status**
14	**Internal Control.** Classifies key spreadsheets based on risks and determines appropriate controls.	Non-Monetary	TBD	Unresolved
15	**Internal Control.** Ensures confidentially and integrity of data and calculations within high-risk spreadsheets.	Non-Monetary	TBD	Unresolved
16	**Internal Control, Economy and Efficiency.** Reduces the risk of unauthorized returns or disclosure due to inappropriate eTSC access.	Non-Monetary	TBD	Open
17	**Internal Control.** Ensures eTSC user accounts are disabled after extended periods of dormancy thus reducing the risk of inappropriate access.	Non-Monetary	TBD	Unresolved
18	**Internal Control.** Ensures unauthorized changes are not introduced into the production software environment.	Non-Monetary	4/5/2013	Closed

EXHIBIT B: OCFO'S RESPONSE TO THE DRAFT REPORT



GOVERNMENT OF THE DISTRICT OF COLUMBIA
OFFICE OF THE CHIEF FINANCIAL OFFICER

Natwar M. Gandhi
Chief Financial Officer

April 5, 2013

Charles J. Willoughby
Inspector General
Office of the Inspector General
717 14th Street, N.W.
Washington, D.C. 20005

Dear Mr. Willoughby:

The following contains the management responses to the findings and recommendations contained in the Office of the Inspector General's (OIG) *Application Control Review of the Integrated Tax System* (OIG No. 11-1-11AT), outlining actions taken or planned, target dates for completion of planned actions and reasons for any disagreements with the findings or recommendations.

The draft report, dated February 25, 2013, contained 18 recommendations related to four findings: Information Technology Strategic Plan, Application Support, Application Controls and General Controls.

FINDING 1: INFORMATION TECHNOLOGY STRATEGIC PLAN

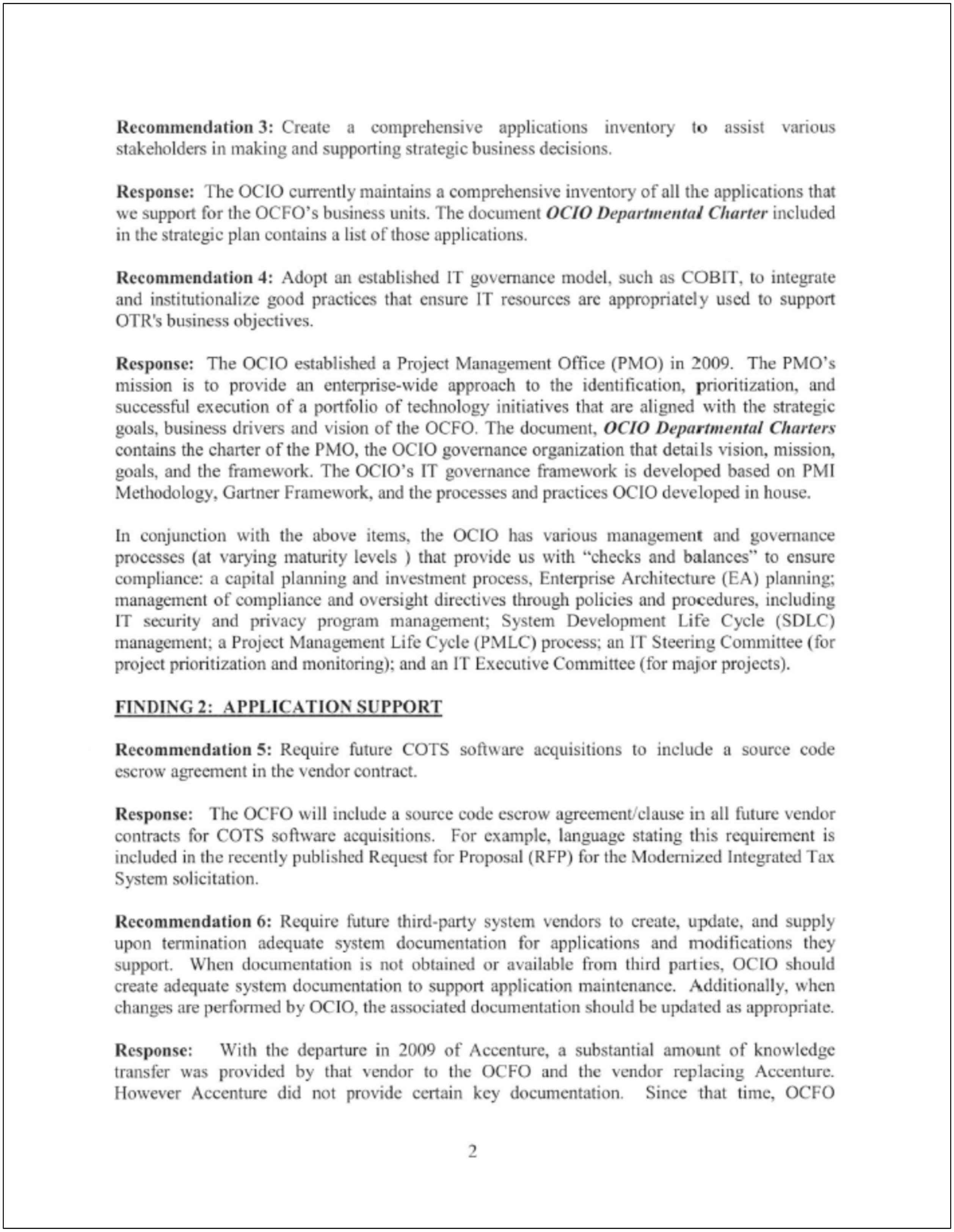
Recommendation 1: Develop and maintain an IT strategic plan aligned with Office of Tax and Revenue's (OTR) strategic objectives.

Response: The Office of the Chief Information Officer (OCIO) developed an IT strategic plan. This plan documents the alignment of the OCIO's goals and objectives with the OCFO's Guiding Principles, which include OTR's strategic objectives. This document will be reviewed and updated annually. We have attached a copy of OCFO IT Strategic Plan 2012-2017.

Recommendation 2: Continue to develop and implement an IT process framework that will accommodate the development and maintenance of an IT strategic plan.

Response: The OCIO currently has a process in place to evaluate initiatives on a quarterly basis to make sure that projects are on track and aligned with the OCIO goals and objectives. The results of these quarterly evaluations are reviewed annually to update the strategic plan, ensuring that alignment with OCFO's business objectives is maintained.

EXHIBIT B: OCFO'S RESPONSE TO THE DRAFT REPORT



Recommendation 3: Create a comprehensive applications inventory to assist various stakeholders in making and supporting strategic business decisions.

Response: The OCIO currently maintains a comprehensive inventory of all the applications that we support for the OCFO's business units. The document ***OCIO Departmental Charter*** included in the strategic plan contains a list of those applications.

Recommendation 4: Adopt an established IT governance model, such as COBIT, to integrate and institutionalize good practices that ensure IT resources are appropriately used to support OTR's business objectives.

Response: The OCIO established a Project Management Office (PMO) in 2009. The PMO's mission is to provide an enterprise-wide approach to the identification, prioritization, and successful execution of a portfolio of technology initiatives that are aligned with the strategic goals, business drivers and vision of the OCFO. The document, ***OCIO Departmental Charters*** contains the charter of the PMO, the OCIO governance organization that details vision, mission, goals, and the framework. The OCIO's IT governance framework is developed based on PMI Methodology, Gartner Framework, and the processes and practices OCIO developed in house.

In conjunction with the above items, the OCIO has various management and governance processes (at varying maturity levels) that provide us with "checks and balances" to ensure compliance: a capital planning and investment process, Enterprise Architecture (EA) planning; management of compliance and oversight directives through policies and procedures, including IT security and privacy program management; System Development Life Cycle (SDLC) management; a Project Management Life Cycle (PMLC) process; an IT Steering Committee (for project prioritization and monitoring); and an IT Executive Committee (for major projects).

FINDING 2: APPLICATION SUPPORT

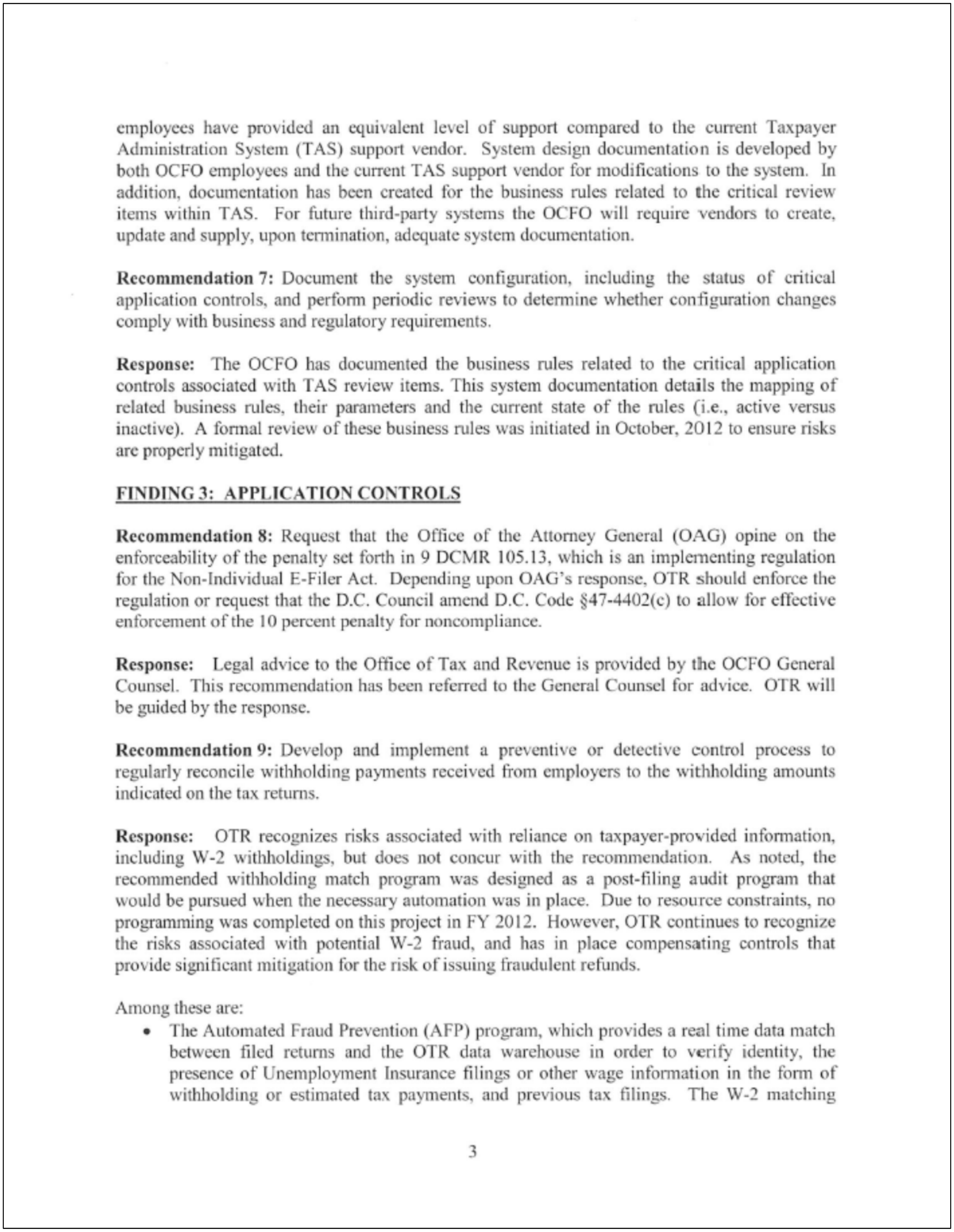
Recommendation 5: Require future COTS software acquisitions to include a source code escrow agreement in the vendor contract.

Response: The OCFO will include a source code escrow agreement/clause in all future vendor contracts for COTS software acquisitions. For example, language stating this requirement is included in the recently published Request for Proposal (RFP) for the Modernized Integrated Tax System solicitation.

Recommendation 6: Require future third-party system vendors to create, update, and supply upon termination adequate system documentation for applications and modifications they support. When documentation is not obtained or available from third parties, OCIO should create adequate system documentation to support application maintenance. Additionally, when changes are performed by OCIO, the associated documentation should be updated as appropriate.

Response: With the departure in 2009 of Accenture, a substantial amount of knowledge transfer was provided by that vendor to the OCFO and the vendor replacing Accenture. However Accenture did not provide certain key documentation. Since that time, OCFO

EXHIBIT B: OCFO'S RESPONSE TO THE DRAFT REPORT



employees have provided an equivalent level of support compared to the current Taxpayer Administration System (TAS) support vendor. System design documentation is developed by both OCFO employees and the current TAS support vendor for modifications to the system. In addition, documentation has been created for the business rules related to the critical review items within TAS. For future third-party systems the OCFO will require vendors to create, update and supply, upon termination, adequate system documentation.

Recommendation 7: Document the system configuration, including the status of critical application controls, and perform periodic reviews to determine whether configuration changes comply with business and regulatory requirements.

Response: The OCFO has documented the business rules related to the critical application controls associated with TAS review items. This system documentation details the mapping of related business rules, their parameters and the current state of the rules (i.e., active versus inactive). A formal review of these business rules was initiated in October, 2012 to ensure risks are properly mitigated.

FINDING 3: APPLICATION CONTROLS

Recommendation 8: Request that the Office of the Attorney General (OAG) opine on the enforceability of the penalty set forth in 9 DCMR 105.13, which is an implementing regulation for the Non-Individual E-Filer Act. Depending upon OAG's response, OTR should enforce the regulation or request that the D.C. Council amend D.C. Code §47-4402(c) to allow for effective enforcement of the 10 percent penalty for noncompliance.

Response: Legal advice to the Office of Tax and Revenue is provided by the OCFO General Counsel. This recommendation has been referred to the General Counsel for advice. OTR will be guided by the response.

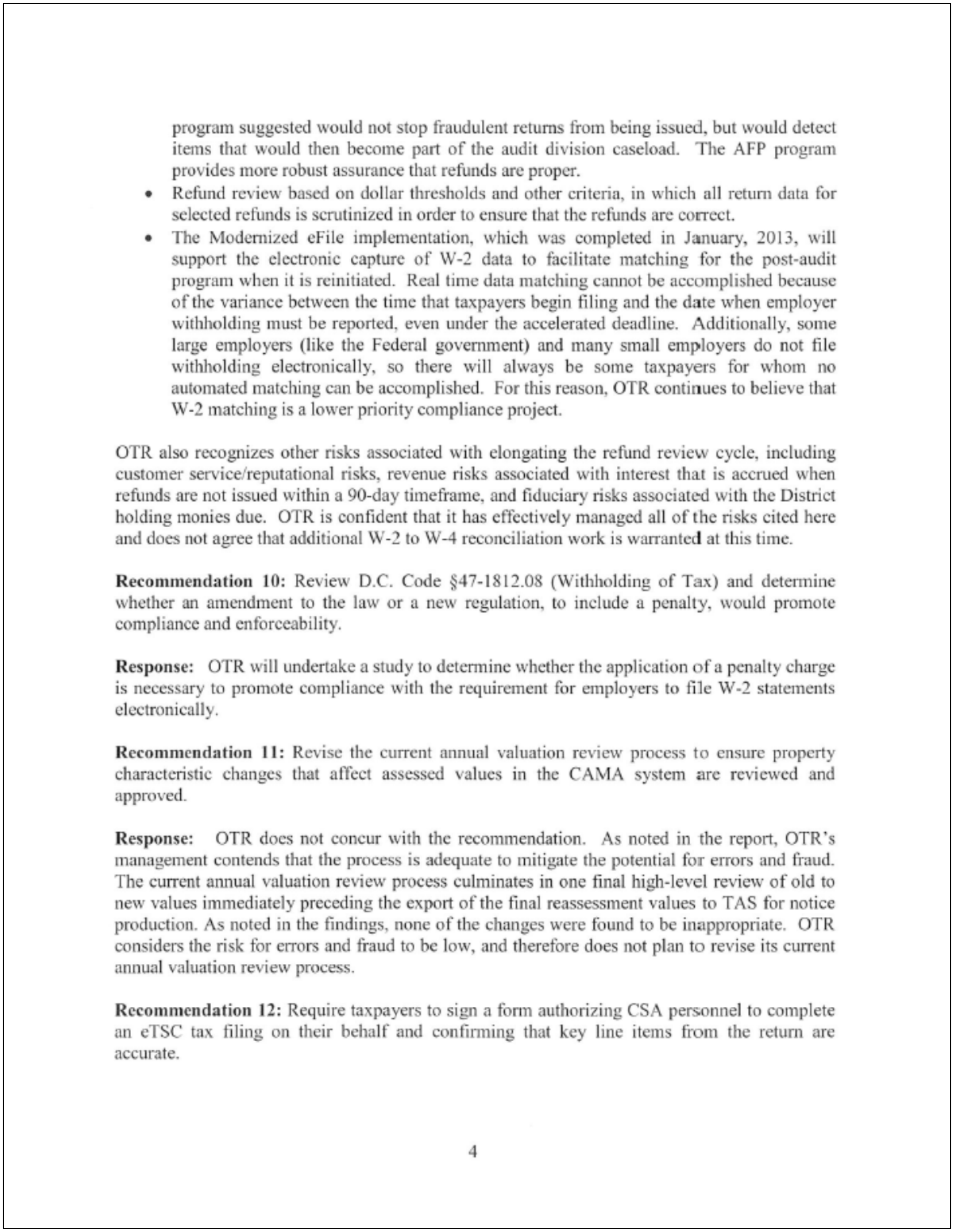
Recommendation 9: Develop and implement a preventive or detective control process to regularly reconcile withholding payments received from employers to the withholding amounts indicated on the tax returns.

Response: OTR recognizes risks associated with reliance on taxpayer-provided information, including W-2 withholdings, but does not concur with the recommendation. As noted, the recommended withholding match program was designed as a post-filing audit program that would be pursued when the necessary automation was in place. Due to resource constraints, no programming was completed on this project in FY 2012. However, OTR continues to recognize the risks associated with potential W-2 fraud, and has in place compensating controls that provide significant mitigation for the risk of issuing fraudulent refunds.

Among these are:

- The Automated Fraud Prevention (AFP) program, which provides a real time data match between filed returns and the OTR data warehouse in order to verify identity, the presence of Unemployment Insurance filings or other wage information in the form of withholding or estimated tax payments, and previous tax filings. The W-2 matching

EXHIBIT B: OCFO'S RESPONSE TO THE DRAFT REPORT



program suggested would not stop fraudulent returns from being issued, but would detect items that would then become part of the audit division caseload. The AFP program provides more robust assurance that refunds are proper.

- Refund review based on dollar thresholds and other criteria, in which all return data for selected refunds is scrutinized in order to ensure that the refunds are correct.
- The Modernized eFile implementation, which was completed in January, 2013, will support the electronic capture of W-2 data to facilitate matching for the post-audit program when it is reinitiated. Real time data matching cannot be accomplished because of the variance between the time that taxpayers begin filing and the date when employer withholding must be reported, even under the accelerated deadline. Additionally, some large employers (like the Federal government) and many small employers do not file withholding electronically, so there will always be some taxpayers for whom no automated matching can be accomplished. For this reason, OTR continues to believe that W-2 matching is a lower priority compliance project.

OTR also recognizes other risks associated with elongating the refund review cycle, including customer service/reputational risks, revenue risks associated with interest that is accrued when refunds are not issued within a 90-day timeframe, and fiduciary risks associated with the District holding monies due. OTR is confident that it has effectively managed all of the risks cited here and does not agree that additional W-2 to W-4 reconciliation work is warranted at this time.

Recommendation 10: Review D.C. Code §47-1812.08 (Withholding of Tax) and determine whether an amendment to the law or a new regulation, to include a penalty, would promote compliance and enforceability.

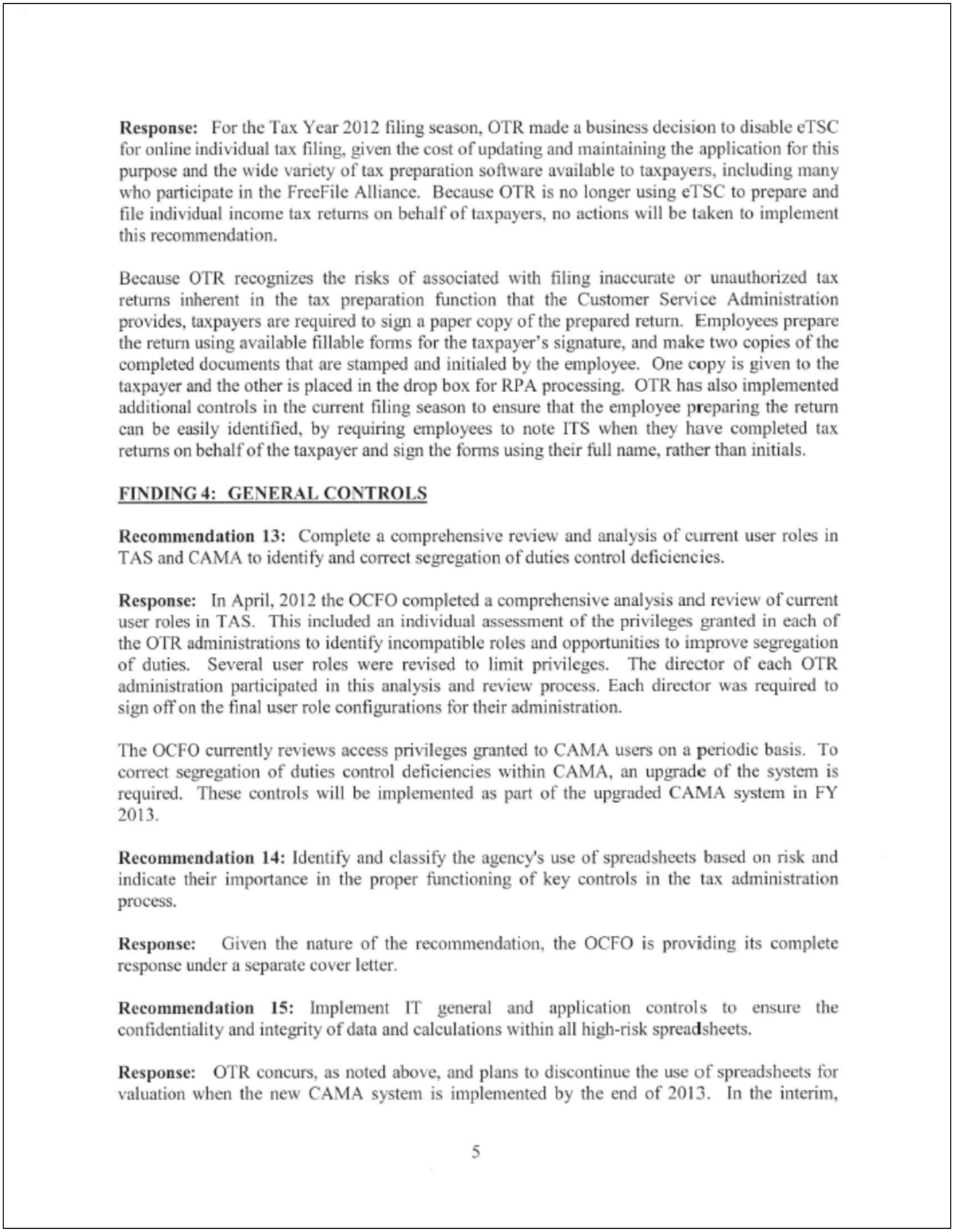
Response: OTR will undertake a study to determine whether the application of a penalty charge is necessary to promote compliance with the requirement for employers to file W-2 statements electronically.

Recommendation 11: Revise the current annual valuation review process to ensure property characteristic changes that affect assessed values in the CAMA system are reviewed and approved.

Response: OTR does not concur with the recommendation. As noted in the report, OTR's management contends that the process is adequate to mitigate the potential for errors and fraud. The current annual valuation review process culminates in one final high-level review of old to new values immediately preceding the export of the final reassessment values to TAS for notice production. As noted in the findings, none of the changes were found to be inappropriate. OTR considers the risk for errors and fraud to be low, and therefore does not plan to revise its current annual valuation review process.

Recommendation 12: Require taxpayers to sign a form authorizing CSA personnel to complete an eTSC tax filing on their behalf and confirming that key line items from the return are accurate.

EXHIBIT B: OCFO'S RESPONSE TO THE DRAFT REPORT



Response: For the Tax Year 2012 filing season, OTR made a business decision to disable eTSC for online individual tax filing, given the cost of updating and maintaining the application for this purpose and the wide variety of tax preparation software available to taxpayers, including many who participate in the FreeFile Alliance. Because OTR is no longer using eTSC to prepare and file individual income tax returns on behalf of taxpayers, no actions will be taken to implement this recommendation.

Because OTR recognizes the risks of associated with filing inaccurate or unauthorized tax returns inherent in the tax preparation function that the Customer Service Administration provides, taxpayers are required to sign a paper copy of the prepared return. Employees prepare the return using available fillable forms for the taxpayer's signature, and make two copies of the completed documents that are stamped and initialed by the employee. One copy is given to the taxpayer and the other is placed in the drop box for RPA processing. OTR has also implemented additional controls in the current filing season to ensure that the employee preparing the return can be easily identified, by requiring employees to note ITS when they have completed tax returns on behalf of the taxpayer and sign the forms using their full name, rather than initials.

FINDING 4: GENERAL CONTROLS

Recommendation 13: Complete a comprehensive review and analysis of current user roles in TAS and CAMA to identify and correct segregation of duties control deficiencies.

Response: In April, 2012 the OCFO completed a comprehensive analysis and review of current user roles in TAS. This included an individual assessment of the privileges granted in each of the OTR administrations to identify incompatible roles and opportunities to improve segregation of duties. Several user roles were revised to limit privileges. The director of each OTR administration participated in this analysis and review process. Each director was required to sign off on the final user role configurations for their administration.

The OCFO currently reviews access privileges granted to CAMA users on a periodic basis. To correct segregation of duties control deficiencies within CAMA, an upgrade of the system is required. These controls will be implemented as part of the upgraded CAMA system in FY 2013.

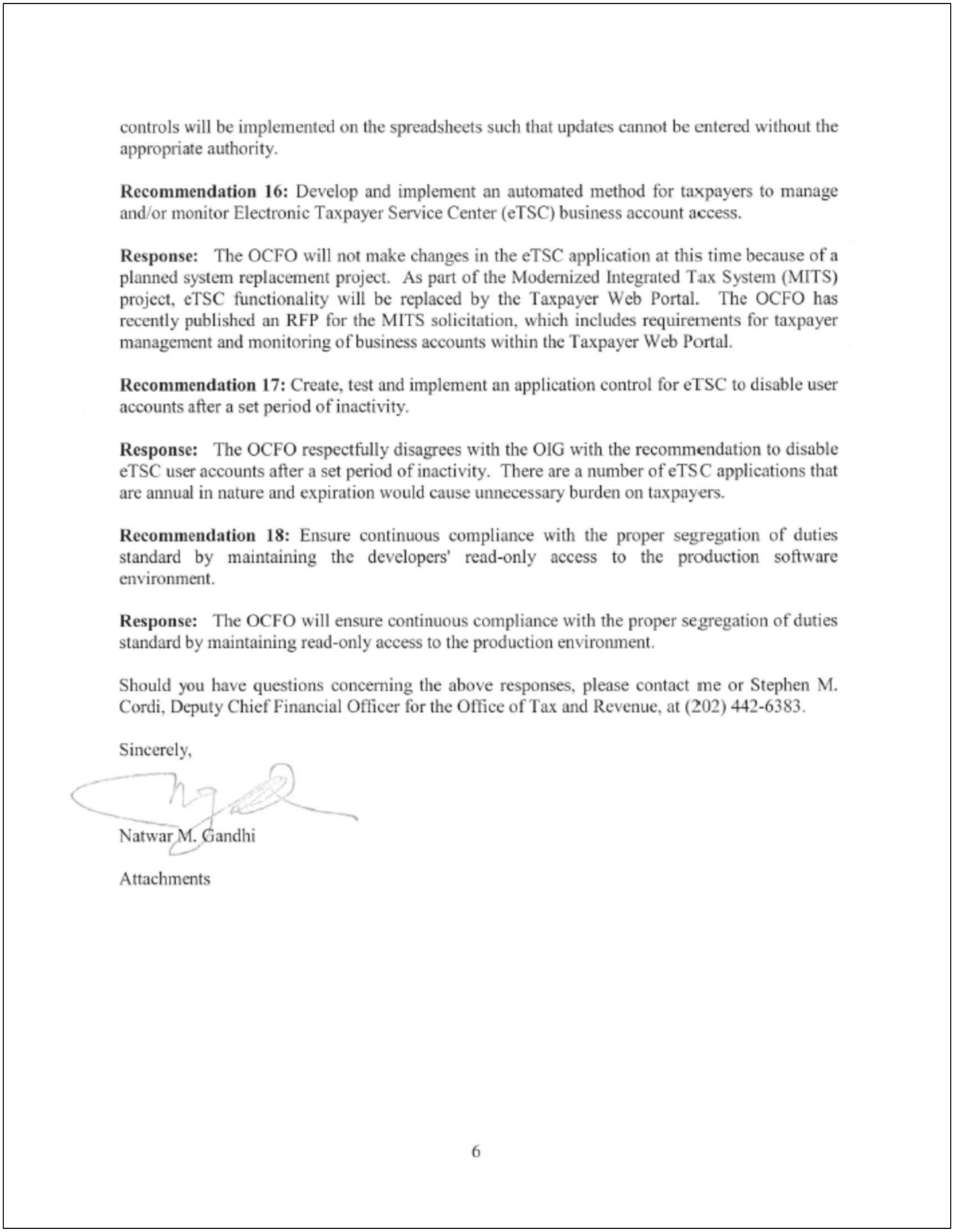
Recommendation 14: Identify and classify the agency's use of spreadsheets based on risk and indicate their importance in the proper functioning of key controls in the tax administration process.

Response: Given the nature of the recommendation, the OCFO is providing its complete response under a separate cover letter.

Recommendation 15: Implement IT general and application controls to ensure the confidentiality and integrity of data and calculations within all high-risk spreadsheets.

Response: OTR concurs, as noted above, and plans to discontinue the use of spreadsheets for valuation when the new CAMA system is implemented by the end of 2013. In the interim,

EXHIBIT B: OCFO'S RESPONSE TO THE DRAFT REPORT



controls will be implemented on the spreadsheets such that updates cannot be entered without the appropriate authority.

Recommendation 16: Develop and implement an automated method for taxpayers to manage and/or monitor Electronic Taxpayer Service Center (eTSC) business account access.

Response: The OCFO will not make changes in the eTSC application at this time because of a planned system replacement project. As part of the Modernized Integrated Tax System (MITS) project, eTSC functionality will be replaced by the Taxpayer Web Portal. The OCFO has recently published an RFP for the MITS solicitation, which includes requirements for taxpayer management and monitoring of business accounts within the Taxpayer Web Portal.

Recommendation 17: Create, test and implement an application control for eTSC to disable user accounts after a set period of inactivity.

Response: The OCFO respectfully disagrees with the OIG with the recommendation to disable eTSC user accounts after a set period of inactivity. There are a number of eTSC applications that are annual in nature and expiration would cause unnecessary burden on taxpayers.

Recommendation 18: Ensure continuous compliance with the proper segregation of duties standard by maintaining the developers' read-only access to the production software environment.

Response: The OCFO will ensure continuous compliance with the proper segregation of duties standard by maintaining read-only access to the production environment.

Should you have questions concerning the above responses, please contact me or Stephen M. Cordi, Deputy Chief Financial Officer for the Office of Tax and Revenue, at (202) 442-6383.

Sincerely,

Natwar M. Gandhi

Attachments