

Secretary of State Audit Report

Kate Brown, Secretary of State

Gary Blackmer, Director, Audits Division



Department of Revenue Computer Controls Ensured Accurate Processing of Tax Returns

Summary

The Oregon Department of Revenue (department) is responsible for administering over 30 taxes for the State of Oregon, including the State's Personal Income Tax and Corporate Excise and Income Tax. Revenues from these sources comprised over 90 percent of the state's General Fund during state fiscal year (FY) 2010, including approximately \$5 billion in Personal Income Tax and \$377 million in Corporate Excise and Income Tax.

The department depends on several computer systems to process Personal and Corporate income tax returns and tax withholding payments. These applications were developed and are maintained by the department's computer programmers and other technical staff.

The purpose of this audit was to evaluate the effectiveness of key general and application controls over the department's computing environment. Based on the results of this work, we found:

- Application controls for the various systems ensured complete and accurate processing of Personal Income and Corporate Tax receipts and refunds.
- Controls over computer code modifications were adequate, but should be improved to better ensure system changes are appropriate.
- Security measures were adequate, but could be improved.

These controls provided reasonable assurance that Personal and Corporate tax transactions were appropriately processed for state Fiscal Year (FY) 2010.

We recommend the department revise its procedures regarding application source code, and address some security matters we describe in a confidential management letter. Our detailed audit recommendations follow the Audit Results section.

Agency Response

The agency response is attached at the end of the report.

Background

The Oregon Department of Revenue (department) is responsible for administering over 30 taxes for the State of Oregon, including the State's Personal Income Tax and Corporate Excise and Income Tax. Revenue from these two taxes comprised over 90 percent of the state's General Fund during state fiscal year (FY) 2010, including approximately \$5 billion in Personal Income Tax and \$377 million in Corporate Excise and Income Tax.

The department depends on several computer systems to process Personal and Corporate income tax returns and tax withholding payments. These applications were developed and are maintained by department computer programmers and other technical staff. In addition, these systems receive related taxpayer inputs from external sources, such as the federal Internal Revenue Service and the Oregon Employment Department.

The department's computer applications are hosted at the Department of Administrative Services' State Data Center (SDC). The SDC is comprised of a complex and extensive inventory of computer operating system platforms, networks, and associated enterprise security infrastructure. Department staff collaborates with the SDC to provide security for confidential taxpayer information and to ensure that computer processing occurs as intended.

Department computer systems that process tax returns generally transfer their outputs to the department's Integrated Tax Accounting (ITA) system. ITA aggregates and manages information from all tax processing systems and supports a database of taxpayer account information. Department accountants use outputs from ITA to manually generate the necessary financial accounting transactions that they post to the state's Statewide Financial Management Application (SFMA). This information is a significant and material ingredient in the state's Comprehensive Annual Financial Report.

The purpose of this audit was to evaluate controls governing the department's information systems that process Individual and Corporate tax returns. Our specific audit objectives were to determine whether information system controls governing these systems provide reasonable assurance that:

- Personal and corporate tax receipt and refund transactions remain complete, accurate, and valid during information input, processing, and output;
- computer code modifications follow appropriate change management processes; and
- systems and data are protected against unauthorized use, disclosure, modification, damage, or loss.

Audit Results

The department relies on various automated and manual computer application controls to ensure outputs of its computer systems are complete, accurate and valid. The effectiveness of these application controls depends on security measures to protect the systems and data, and program change management procedures to ensure program code modifications are strictly controlled.

We evaluated these key computer controls governing the applications the department uses to process Individual and Corporate income taxes, and found:

- Application controls for the various systems ensured complete and accurate processing of Personal Income and Corporate Tax receipts and refunds.
- Controls over computer code modifications were adequate, but should be improved to better ensure system changes are appropriate.
- Security measures were in place to protect department computer systems, but could be improved.

Based on these results, we concluded that the department's computer controls provided reasonable assurance that Personal and Corporate tax transaction amounts processed through department systems during state fiscal year 2010 were complete, accurate and valid. We did note that source code and security procedures could be improved.

Application Controls Ensured Complete and Accurate Processing of Personal Income and Corporate Tax Receipts and Refunds

Effective application controls include both manual and automated processes to ensure only complete, accurate, and valid information is entered into a computer system; data integrity is maintained during processing; and system outputs conform to anticipated results. The key application controls the department has in place to ensure these attributes are achieved for tax returns processed through its systems included automated and manual data validity checks, transaction balancing routines, and error detection and correction processes.

Data validity checks ensured valid inputs

The department receives Personal and Corporate Tax data from paper documents, such as hard copy tax returns, and digital files transferred from other systems. Controlling and validating these data inputs is critical to ensuring the integrity and completeness of computer processing.

The department ensures manually entered tax data accurately reflects hard copy documents by double-keying the information into the system. For this process, two individuals independently enter the same data into a file where the computer compares them. If the two inputs are identical, the system accepts a copy of the transaction. Should the inputs not match, the differences are investigated and resolved, and a correct copy is accepted into the system.

Department computer systems automatically validate data received electronically to ensure they are complete and conform to required formats. Files coming from other systems, such as employer quarterly withholding data, are automatically rejected if they do not contain required information fields or a specified number of records. Tax returns received electronically are also evaluated by the systems to ensure transmissions are complete before they are accepted for processing.

Error detection and correction routines ensure correct processing

During data processing, department systems apply a variety of automated logical checks to ensure Personal and Corporate Tax return data remain complete, conform to required parameters, and are mathematically correct. Automated controls also monitor system processes to ensure batches complete the required processing steps.

Should an application detect an anomaly while processing tax returns, department systems are designed to either halt further processing of the entire batch or suspend processing of a specific return until the conditions are resolved. In either case, department applications generate error reports that are routed to designated and experienced staff who make the necessary adjustments or corrections to allow processing to continue.

Transaction balancing routines ensured processing completeness

Department staff uniquely label and secure hard document returns during the data validation and input. In addition, they use sign off sheets to ensure required processing steps occur before returns are accepted for processing. System applications utilize supplemental

information included at the beginning of electronic files to ensure they remain complete as they are transferred between systems and system processes.

Code Modification Controls Were Adequate, But Should Be Improved to Better Ensure System Changes Are Appropriate

Mainframe computer programs are generally written using a programming language such as Java or Cobol. These languages allow programmers to write understandable statements, referred to as source code, that represent the actions a programmer wants the computer to take. Source code must be translated or compiled into a much more cryptic form, called object or binary code, before it can actually run on a computer.

Generally accepted computer control standards indicate that program source and object code should be strictly managed to ensure only tested and approved modifications are compiled and implemented in production. To ensure this occurs, logical access to code should be strictly limited and monitored. In addition, proposed changes to code should be independently tested and compared to the latest version of authorized code to ensure only appropriate modifications are made.

The department has procedures in place to manage code modifications to computer applications. These practices included processes for authorizing changes, testing proposed modifications, approving code changes, and strictly limiting access to production object code. However, the department has not implemented procedures to strictly control application source code prior to its compilation to object code and graduation to production. Specific weaknesses include:

- The department's application programmers have full logical access to the source code libraries, contrary to best practices.
- Department staffs do not routinely compare proposed source code modifications to the latest authorized versions to ensure only authorized changes were made.
- Changes to source code and movement of source and object code is logged, but department staff does not routinely review the logs.
- The software tool department personnel use to implement code has software version control features to track changes to code, but these features are not enabled.

- Staff assigned to move code to production does not routinely confirm the changes were authorized and approved by management.

These weaknesses increase the risk that department programmers could introduce unauthorized and untested changes to computer applications. Should this occur, the department could experience costly delays or errors in processing Individual and Corporate Income tax returns.

During our review, we noted that the weaknesses were likely the result of management's long-standing trust in its experienced team of system developers. In addition, at the time we completed our fieldwork, the department was implementing more robust program change control policies and procedures.

Security Measures Protected Department Computer Systems, But Could Be Improved

One of our objectives was to determine whether system information was protected against unauthorized use, disclosure, modification, damage or loss. We found that security measures were in place to protect department computer applications. However, we noted some weaknesses that should be corrected.

Because of its sensitive nature, we excluded detailed information relating to security findings and recommendations from this report. That information will be communicated to the department under separate cover in accordance with ORS 192.501 (23), which exempts sensitive information from public disclosure.

Recommendations

To better control changes to applications, we recommend the department:

- Strictly limit and monitor programmers' access to the application source code libraries.
- Establish procedures for comparing proposed source code modifications to the latest authorized versions.
- Ensure systems logs depicting movement of source and object code are routinely reviewed.
- Consider enabling version control features included in the "Implementer", the department's software implementation tool.
- Ensure staff routinely confirms that software changes are authorized and approved by management before moving code to production.

To improve security, we recommend the department implement the recommendations included in our confidential management letter.

Objectives, Scope and Methodology

The purpose of this audit was to review and evaluate the effectiveness of key general and application controls over the computing environment at the department. Our primary audit objectives were to determine whether information system controls governing these systems provide reasonable assurance that:

- Personal and corporate tax receipt and refund transactions remain complete, accurate, and valid during information input, processing, and output;
- computer code modifications follow appropriate change management processes; and
- systems and data are protected against unauthorized use, disclosure, modification, damage, or loss.

To meet these objectives, we conducted interviews with appropriate department personnel and observed department operations and processes. In addition, we examined technical documentation relating to information processing and system architecture.

To evaluate system application controls over tax return transactions, we reviewed whether:

- Control totals were utilized to ensure that all transactions input were also processed;
- applications performed calculation and validation checks against data being processed; and
- system logs were used to identify and resolve errors.

To test program change management controls, we evaluated the department's change management policies and procedures and performed a limited review of supporting documentation for selected changes.

To determine whether systems and data were reasonably secure, we:

- Reviewed department security policies and procedures;
- reviewed logical access listings, access policies, and the related system parameters; and
- tested for continued system access for employees that had been terminated from the department.

We used the United States Government Accountability Office's publication "Federal Information System Controls Audit Manual"

(FISCAM) to identify generally accepted control objectives and practices for information systems.

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.



Oregon

John A. Kitzhaber, MD, Governor

Department of Revenue

955 Center St NE

Salem, OR 97301-2555

www.oregon.gov/dor

July 20, 2011

Gary Blackmer, Director
Secretary of State, Audits Division
255 Capital Street NE, Suite 500
Salem, OR 97301

Dear Mr. Blackmer,

This letter is our management response to the audit report on the Department of Revenue Computer Controls Ensured Accurate Processing of Tax Returns. We appreciate the professional and collaborative manner in which the Secretary of State staff performed this audit.

The findings and recommendations within the draft report provide insight into the challenges associated with applying current security practices to legacy systems. We are grateful for the information provided and believe that it validates our position that the core systems that process our highly complex tax programs need to be replaced.

Please accept the following comments on the recommendations contained in the report:

Recommendation:

Strictly limit and monitor programmers' access to the application source code libraries.

Response:

We agree – Revenue is looking into additional controls for limiting and monitoring programmers' access with the current tools we have available. At the same time, we are preparing to document the mitigating controls that help enforce version control for source code.

Recommendation:

Establish procedures for comparing proposed source code modifications to the latest authorized versions.

Response:

We agree - Revenue is in the process of formalizing existing processes.



Recommendation:

Ensure system logs depicting movement of source and object code is routinely reviewed.

Response:

We agree – A system log exists; we will create a procedure to routinely review system logs depicting movement of source and object code.

Recommendation:

Consider enabling version control features included in the "Implementer", the department's implementation tool.

Response:

We agree - we are looking into the features and functionality of the Implementer and whether or not we can safely turn this feature on.

Recommendation:

Ensure staff routinely confirms that software changes are authorized and approved by management before moving code to production.

Response:

We agree – The Change Advisory Board (CAB) process requires that changes be reviewed. Production Control is responsible for promotion to production and a Production Control member sits on CAB. If an analyst requests a move without checking CAB for approval, it should be caught by Production Control.

Recommendation:

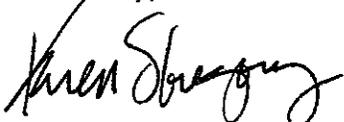
To improve security, we recommend the department implement the recommendations included in our confidential management letter.

Response:

Revenue agrees with the recommendations within the confidential management letter and will begin implementing the specific responses.

Thank you for the opportunity to respond.

Sincerely,



Karen S. Gregory, Acting Director
Department of Revenue
955 Center St NE
Salem, OR 97301-2555

About the Secretary of State Audits Division

The Oregon Constitution provides that the Secretary of State shall be, by virtue of her office, Auditor of Public Accounts. The Audits Division exists to carry out this duty. The division reports to the elected Secretary of State and is independent of the Executive, Legislative, and Judicial branches of Oregon government. The division audits all state officers, agencies, boards, and commissions and oversees audits and financial reporting for local governments.

Audit Team

William K. Garber, CGFM, MPA, Deputy Director

Neal E. Weatherspoon, CPA, CISA, CISSP, Audit Manager

Mark A. Winter, CPA, CISA, Principal Auditor

Glen D. Morrison, MBA, CISA, Staff Auditor

This report, a public record, is intended to promote the best possible management of public resources. Copies may be obtained from:

internet: <http://www.sos.state.or.us/audits/index.html>

phone: 503-986-2255

mail: Oregon Audits Division
255 Capitol Street NE, Suite 500
Salem, OR 97310

The courtesies and cooperation extended by officials and employees of the Department of Revenue during the course of this audit were commendable and sincerely appreciated.