

Secretary of State **AUDIT REPORT**

Report No. 2003-14 • April 15, 2003

Oregon Department of Revenue: Corporation Automatic Tax— Application Controls Review



Bill Bradbury, Secretary of State
Cathy Pollino, Director, Audits Division

Summary

PURPOSE

The purpose of this audit was to evaluate whether data processed by the Department of Revenue's Corporation Automatic Tax (CAT) system remained complete, accurate and valid throughout the data management process, and to evaluate the processes used for systems development and ongoing maintenance, physical and logical security, and disaster recovery and contingency planning. We also conducted a follow up on prior audit findings.

RESULTS IN BRIEF

We determined that the Department of Revenue's Corporation Automatic Tax (CAT) system generally maintained the completeness, accuracy and validity of the data; however, we did find several minor programming errors warranting management's attention. We also found that processes relating to systems development and maintenance activities, physical and logical security, and disaster recovery and contingency planning could be improved. Finally, we found that the department fully implemented three of 15 prior audit recommendations.

RECOMMENDATIONS

We recommend that the department:

- Formalize its stated controls in policy and procedures regarding data entry and verification of returns.
- Consider modifying its batch processing system to further enhance the data input edit routines.

- Correct the programming and processing errors identified in this report and refund overpayments resulting from those errors.
- Further develop, implement, and enforce systems development and maintenance methodologies, including emergency change procedures and independent reviews.
- Limit and closely monitor programmers' access in the production environment.
- Improve logical access by enforcing its existing security policies and removing unneeded system access.
- Make physical security a higher priority.
- Fully develop disaster recovery and business continuity plans and improve its offsite storage facility controls.
- Re-evaluate and formalize its processes for establishing tolerance levels.
- Implement prior audit recommendations that have not been fully resolved.

AGENCY'S RESPONSE

Department of Revenue management generally agrees with the recommendations and has either taken, or will take, steps to address them.

Background

The Department of Revenue (department) relies on numerous computer applications to administer more than 30 tax programs. One of these applications is the Corporation Automatic Tax (CAT) system, which processes over 90,000 corporation tax returns each year.

The department developed CAT internally and placed it into production in August 1997. Since its implementation, CAT has undergone numerous enhancements and modifications due to changes in tax laws and user needs.

The department's Information Processing Division Computer Services Section is responsible for providing an appropriately secure operating environment for its systems.

Information System Controls

Information system controls are typically classified as general controls or application controls. General controls protect the environment in which software applications process data. Application controls relate to

specific processing requirements of individual software applications. They are designed to reduce the risk of errors in recording, processing, classifying or summarizing transactions. General controls coupled with application controls provide more assurance that transactions processed through the system are authorized, reliable and complete.

Audit Results

Application Controls

Application controls include methods of ensuring that: only

complete, accurate, and valid data are entered in a computer system; processing performs the correct functions and results are accurate; and data are properly maintained. Those controls can be either manual or automated processes.

We reviewed the department's processes and controls over data preparation, input, processing, output and storage relating to the CAT system. Although we determined that the CAT system generally maintained the completeness, accuracy and validity of the data, we identified several minor programming errors in the area of data input and processing that warrant management's attention.

Data Input

Controls over data input ensure that input errors are detected, reported and corrected prior to processing and as close to origination of the error as possible. The department enters taxpayer information into CAT by either batch processing or direct input into the system. We tested the department's points of entry to determine if controls were working.

Although the direct input method correctly detected and reported input errors, the batch entry method did not report an error when an incorrect future date was entered. In addition, the batch processing system allowed the same individual to enter and verify taxpayer information when the department's stated control is that the same person will not perform both functions.

We recommend that management formalize its stated controls in policy and procedures for data entry and verification of returns.

Agency's Response:

Management agrees. Prior to the next processing season beginning January 2004, management will formalize stated controls in policy

and procedures for data entry and verification of return information.

We also recommend that management consider modifying its batch entry system or develop compensating controls to:

- Account for incorrect future dates, and
- Prohibit the same employee from both entering and verifying data.

Agency's Response:

Management agrees. Management is currently developing requirements for software that will have compensating controls that will prevent or correct the entry of incorrect future dates and prohibit the same employee from both entering and verifying the data. Acquisition of software is contingent upon funding.

Data Processing

Controls over data processing ensure that all data that has been input is correctly processed and conforms to predetermined criteria. The department relies on various automated routines to meet its processing objectives. For example, CAT examines the tax year start and end date to ensure that the taxpayer is filing for a valid period.

We tested some of the key CAT processing routines and noted the following weaknesses:

- Due to programming errors, the required number of supervisory approvals on tax refunds over certain dollar amounts did not always occur.
- One relational edit routine intended to ensure the accuracy of the data did not function as intended.
- One routine designed to allow processing to continue without explanation or correction of the condition resulted in an incorrect calculation of net tax in six of ten returns selected for review. Although two accounts were corrected when the taxpayer filed

an amended return, the other four taxpayers overpaid by a total of \$46,375.

- Control totals generated were not always utilized to ensure that all transactions input were also processed.

We recommend that the department correct the programming and processing errors identified above and refund overpayments resulting from its system errors.

Agency's Response:

Management generally agrees. The programming and processing errors identified in the audit will be corrected within 6 months. The overpayments identified in the audit will be refunded in 45 days, if the law allows.

Systems Development and Change Management

The development of new application systems should be made using a written systematic approach that ensures all phases of systems development are adequately addressed. This approach to programming is called a Systems Development Life Cycle (SDLC) methodology. For ongoing system changes, there should be a similar process followed as with new development. Situations requiring emergency changes should be defined and procedures established to ensure that all controls are retroactively applied, as normal processes are often circumvented. The methodologies should minimize the risk of disruptions, unauthorized alterations and errors to systems.

The Information Processing Division Computer Services Section has an SDLC methodology that outlines tasks to be performed and specifies resulting deliverables during major system development efforts. For example, it requires development of diagrams that include definitions of the proposed system functions, information flow, and data storage requirements. It

also requires delivery of approved detail designs for each subsystem component. For ongoing system maintenance or enhancements, Computer Services uses less complex but similar methodologies.

We tested the department's methodologies and practices to ensure that development efforts were adequately controlled. Testing showed that development staff did not always follow the established methodologies, as not all of the required deliverables were created.

In addition, the department's methodology governing ongoing maintenance did not include some necessary key elements. For example, its methodology did not include:

- Formal management approval prior to work beginning;
- Assessment of the impacts proposed changes may have on other computer systems;
- Documentation of testing plans and results; or
- Processes to update original system source documentation.

Finally, the department did not fully establish and implement emergency change procedures and did not establish procedures requiring independent review of work performed during development and maintenance efforts.

We recommend that Computer Services management ensure that development staff follow its existing methodologies.

Agency's Response:

Management agrees. The Computer Services Section has established a new committee called the Workload Planning Group, which includes systems development managers and team leaders. By September 2003, this group will develop a process to ensure that existing methodologies are followed.

We recommend that Computer Services management fully develop its maintenance processes to include the key elements identified above.

Agency's Response:

Management agrees. The Computer Services Section has established a new committee called the Workload Planning Group, which includes systems development managers and team leaders. By September 2003, this group will enhance Computer Services Section maintenance processes.

We recommend that Computer Services management establish and implement procedures over emergency changes. Such procedures should define what constitutes an emergency change and require retroactive application of normal processes and controls including management review and approval.

Agency's Response:

Management agrees and has developed emergency change procedures. We are currently in the process of documenting and implementing them.

We recommend that Computer Services management establish and implement an independent review of development staffs' work. Independent review should ensure that changes made reflect only what was requested and approved, and adhere to development standards.

Agency's Response:

Management agrees with the intent of the recommendation. Current methodology requires that all code changes be reviewed by a systems development analyst who did not code the changes. All changes are thoroughly tested by the developer and by an independent user tester. Our plan is to continue to refine our methodology and ensure that it is followed by development staff.

Logical Access Controls

In order to safeguard information against unauthorized use, disclosure, modification, damage, or loss, logical access controls should ensure that access to systems, data, and programs is restricted to authorized users. Specifically, access should be granted only to those individuals with a demonstrated business need and programmers' access should be limited to a test environment. However, in emergency situations, programmers may be allowed temporary access to the production environment to resolve problems and allow critical processing to continue. Such access should be logged and closely monitored.

The department relies on various manual and automated controls to limit access to its systems. For example, its system is set to force periodic password changes and requires a minimum password length. In addition, the department has established various policies and procedures regarding security.

We tested the department's logical access controls to ensure that access was restricted to authorized users and granted based on an individual's demonstrated need.

Although the department made efforts to further restrict access granted to users, we found areas that could be improved. Specifically, testing showed that programmers had unlimited access to the production environment and used that access to perform routine functions such as changing menu options and granting system access to user groups.

In addition, management did not perform a thorough review of programmers' activities and changes within the production environment.

We also found that the department did not always enforce its established security policies. For example:

- Access was not always limited to an individual's assigned responsibilities. Specifically, computer operators have broad access to the CAT system and some staff were granted access rights to input data but were not assigned data entry responsibilities.
- User access was not always timely deactivated once an employee terminated employment with the department.
- Password resets were not always logged or performed by authorized individuals and some system password parameters were not set as required.
- Internet access approval was not always documented.

As a result, the department is less able to safeguard its systems, data, and programs.

We recommend that Computer Services management limit programmers' access in the production environment to emergency situations and closely monitor those activities.

Agency's Response:

Management agrees with the intent of the recommendation. We have created additional limitations to programmer access and have improved monitoring of when programmers access the production environment. Programmers cannot change program code in production. We have made improvements to the review and documentation process that include review and approval by an independent user tester.

We also recommend that department management enforce its existing security policies as well as remove unneeded access to the CAT system.

Agency's Response:

Management agrees. The department has gone through an extensive process to determine and establish logical AS/400 group

profiles. These profiles are used to grant access to specific information on the AS/400. Those employees who need access to the CAT System, as part of their jobs, are in group profiles that can access the CAT System. Employees who have no need to access the CAT System, as part of their jobs, are in group profiles that do not have access to the system.

Physical Access Controls

The department is responsible for restricting physical access to its building to authorized individuals in order to protect its computer systems and confidential information.

The department relies on various controls to limit physical access to its computer systems and data. Specifically, the department has a designated physical security officer and access within certain areas of the building is controlled by a keycard system, maintained by the Department of Administrative Services (DAS). In addition, all staff and visitors having access to confidential taxpayer information are required to sign a nondisclosure statement agreeing not to disclose confidential information.

We reviewed the department's physical access controls and found that the department could make improvements. Specifically:

- The physical security officer position is periodically rotated among staff. As such, security responsibilities are often neglected. For example, the current and prior security officer did not perform any monitoring functions and did not conduct periodic review and confirmation of individuals having access privileges.
- The department did not adequately restrict physical access to sensitive areas, including the computer services and confidential files sections.

- Of the 70 individuals granted access to the computer room, 58 may not need such access, including various department staff, Oregon State Police, and DAS Facilities. This situation is due in part to other agency management authorizing and issuing key cards without the department's authorization.
- Staff responsible for administering keycards did not always deactivate the cards within one business day after staff terminated employment with the department. For example, it took staff between three and 21 days after the employee's termination date to deactivate nine of 18 key cards selected for testing.
- Although the department requires visitors to sign a nondisclosure statement on an annual basis, it does not for permanent staff. We found that 15 of 20 permanent employees selected for testing had not updated the statement within the last year; seven statements dated back to 1992.

As a result, management is less able to protect its data and systems from unauthorized use, destruction, modification, and disclosure.

We recommend that management ensure that security responsibilities are fulfilled.

Agency's Response:

Management agrees. The department has permanently assigned the duties of Security Officer to the Facilities Coordinator in the Finance Section. The Security Officer duties have been incorporated into the position description.

We recommend that management further restrict access to sensitive areas as identified in this report.

Agency's Response:

Management agrees. The department has reviewed access provided to both agency and non-

agency staff to sensitive areas and has removed access from inappropriate individuals. A quarterly review process of access to sensitive areas is in place, as well as a monthly review of individuals that have actually physically accessed the Computer room using their key card. The review process and the process for granting access to these rooms is documented in Policy and Procedure No. 281-003.

We recommend that management remove unnecessary access.

Agency's Response:

Management agrees. As in the recommendation above, the department will continue to review access and remove access that is determined to be unnecessary.

We recommend that management modify existing procedures to ensure that key cards are deactivated in a timely manner.

Agency's Response:

Management agrees. Procedures have been modified to ensure prompt deactivation of key cards.

We recommend that management require permanent employees to renew the nondisclosure statements annually.

Agency's Response:

Management agrees. We plan to electronically send the agency secrecy clause certificate to all employees on an annual basis. Employees will respond electronically that they have received the information and agree to abide by applicable disclosure laws. We plan to implement this procedure in the fall of 2003.

Disaster Recovery and Contingency Planning

Disaster Recovery and Contingency planning are necessary to ensure that services can be restored in the event of a disruption. These plans should provide detailed instructions for recovery from

various disaster scenarios and be updated and tested on a regular basis.

Although the department has developed some disaster recovery plans, those plans are incomplete and out-of-date and the department has not created business continuity plans. In addition, the department has not conducted testing since February 2000 and its hot site contractor may not be sufficient for the department's needs. These weaknesses have been communicated to the agency during prior audits but continue to exist.

We also noted the following additional weaknesses:

- The department's offsite storage facility is not located far enough away from the department so as not to be affected by the same disaster.
- Not all backup tapes and printouts necessary to facilitate a timely recovery were located at the offsite storage facility.
- The Computer Services Section did not back up all necessary files during the full weekly backup.

In the event of a disaster, the department may be unable to fully recover all of its business operations in a timely manner.

We recommend that management fully develop disaster recovery and business continuity plans.

Agency's Response:

Management agrees with the intent of the recommendation. We have formed an agency-wide business continuity steering committee whose purpose is to guide, direct, and prioritize core business functions in creating and maintaining a business continuity plan. A business continuity manual has been created, including a detailed outline of the essential contents and format of a thorough business continuation plan. The top five functions were prioritized by the steering

committee. Banking was identified as our first priority and a business continuity plan was developed for it. Significant progress has been made in four other business critical areas of Revenue.

We recommend that management put into place a hot site provider that is able to meet its needs and conduct recovery training on a regular basis.

Agency's Response:

Management agrees. The Department of Revenue is one member of a coalition of agencies that has issued an RFP for disaster recovery services. The other agencies are DHS, ODOT, and DAS. Only one response was submitted. The agencies are evaluating the response at this time.

We recommend that management relocate its offsite storage facility to a location that would be less affected by the same disaster, and ensure that all files necessary for recovery of operations are backed up and moved to its off-site storage facility.

Agency's Response:

Management agrees. DOR has organized a disaster recovery development team that is currently addressing the software backup and storage issues. One of the first steps was to acquire a "snap shot" of the backup processes presently being used. That phase (Phase 1) was completed during February 2002. Phase 2 will be to validate that all critical business systems are backed up to a "yet to be determined" standard. Phase 3 will consist of process changes, and Phase 4 will be to make recommendations for any new storage locations and fully test the recovery processes. We expect the relocation of offsite storage to be completed by September 2003.

Other Matters

Corporations are required to pay estimated tax payments on a quarterly basis. When a corporation does not make the necessary

payments in a timely manner, the department may charge interest on the underpayment. The department, however, has established a tolerance level of \$200, which is intended to eliminate excessive administrative costs associated with billing out smaller amounts. Thus, when a corporation owes interest that is less than \$200, the department does not issue a bill.

During the audit, we found that the department was unable to provide justification for the amount of the tolerance level and did not have formal policies and procedures governing the establishment of such tolerance levels. In addition, the department established the \$200 tolerance in 1994, during a time when it relied more on manual processes.

As a result, a total of \$170,803 in interest was not billed to corporations during 2001.

We recommend that the department re-evaluate and formalize its processes for establishing tolerance levels.

Agency's Response:

Management agrees. Prior to the next processing season, beginning January 2004, we will evaluate and formalize a process for establishing tolerance levels and reviewing the tolerance level annually.

Follow Up on Prior Audit Recommendations

This section summarizes the Department of Revenue's efforts to resolve prior audit findings included in our report No. 2000-19 titled *Department of Revenue: Application Controls Review*, June 1, 2000.

The purpose of the audit was to review the controls governing the Integrated Tax Accounting system (ITA). The ITA system provides common functions such as accounting, check writing, billing, and other tax maintenance functions.

This review resulted in 15 findings and recommendations.

Of the 15 recommendations noted in this report, three were resolved relating to ITA output, the department's operations manual, and formal assignment to monitor and update selected tables. However, 12 recommendations remain unresolved. Eight of the recommendations pertain to CAT as well as ITA and are discussed in the body of this report. The remaining four recommendations are discussed below along with management's actions taken since the end of fieldwork date.

Prior Audit Finding

Fully document and monitor compliance with policies and procedures governing who should provide the various levels of transaction review and approval including assignment of automatic transaction approval.

Status—partially resolved.

Agency's Response:

Management agrees. Agency policies and procedures have been updated to reflect processes in place for granting and reviewing transaction review and approval authorities (PAP Nos. 331-002 and 281-246).

Prior Audit Finding

Remove the review authority awarded to inappropriate reviewers identified during our audit including Computer Services employees and the internal auditor.

Status—partially resolved.

Agency's Response:

Management agrees. This review has been completed and authority of inappropriate reviewers has been removed. Policy and Procedure No. 331-002 addresses the ongoing review of this authority.

Prior Audit Finding

Correct the programming error in ITA so that the correct number of reviews will occur for all online adjustments or develop compensating controls to mitigate the risk caused by the error.

Status—partially resolved. The department elected to implement compensating controls; however, those controls did not always work as intended.

Agency's Response:

This correction was made and implemented in August, 2000. It is working as intended. We will look further at the specific examples of concern in the CAT Audit.

Prior Audit Finding

Develop and implement policies and procedures to track, safeguard, and control use of computer equipment costing less than \$5,000. In addition, record and conduct a periodic written inventory of all equipment with higher risk of loss, such as personal computers.

Status—partially resolved. Although the divisions within the department have developed some methods for tracking computer equipment, those methods are inconsistent among divisions and have yet to be formalized.

Agency's Response:

Management agrees. We are currently gathering additional business requirements to develop a formal plan for a single asset management system.

Objectives, Scope and Methodology

The objective of our audit was to evaluate whether data processed by the Department of Revenue's Corporation Automatic Tax system remained complete, accurate and valid throughout the data management process, as well as the processes used for system

development and ongoing maintenance. Those controls included policies and procedures to manage system and programming changes; ensure appropriate data preparation, input, processing, output and storage; provide adequate physical and logical security over its computer systems and data; and provide disaster recovery and contingency planning. We conducted our fieldwork between December 2001 and September 2002.

During our audit we interviewed various department personnel,

examined documents supporting controls and observed various processes and operations. We also evaluated compliance with applicable laws, rules, and regulations pertaining to the CAT system. Finally, we reviewed the status of the department's efforts to resolve control weaknesses identified in our last audit report titled *Department of Revenue: Application Controls Review*, issued June 1, 2000.

During our audit, we used the Information Systems Audit and Control Foundation's (ISACF)

publication "Control Objectives for Information and Related Technology" (COBIT) to identify generally accepted and applicable internal control objectives and practices for information systems. ISACF is a worldwide organization dedicated to research, develop, and publicize control objectives and audit guidelines.

We conducted our audit according to generally accepted government auditing standards.

This report, which is a public record, is intended to promote the best possible management of public resources. Copies may be obtained by mail at Oregon Audits Division, Public Service Building, Salem, Oregon 97310, by phone at 503-986-2255 and 800-336-8218 (hotline), or internet at Audits.Hotline@state.or.us and <http://www.sos.state.or.us/audits/audithp.htm>

AUDIT ADMINISTRATOR: *Nancy L. Young, CPA, CISA*
AUDIT STAFF: *Shandi C. Frederickson, Erika Ungern, Geoff Hill, Rebekah Cole*
DEPUTY DIRECTOR: *Charles A. Hibner, CPA*

The courtesies and cooperation extended by the officials and staff of the Oregon Department of Revenue were commendable and much appreciated.

Auditing to Protect the Public Interest and Improve Oregon Government
