

Secretary of
State
**AUDIT
REPORT**

Report No. 98-12 • May 7, 1998

**Department of Revenue:
General and Personal Income Tax
Application Controls**



Phil Keisling, Secretary of State
John Lattimer, Director, Audits Division

Summary

PURPOSE

The purpose of this audit is to follow up on the findings reported in the 1995 audit of the Department's Information System General and Application Controls. Our review covered the general controls intended to protect the environment in which applications process data, including physical security of the data center, access controls and the controls over developing and modifying applications. It also included a follow up of the prior audit findings specific to the Personal Income Tax application.

BACKGROUND

The department collects 94 percent of the state's general fund revenues through its various tax programs. The department's computerized systems are essential to the tax collection process. Over a period of years, the department has been migrating all tax programs and accounting functions to a single in-house developed system that will be integrated with the department's accounting system. This in-house system will operate on the department's AS/400 computer.

RESULTS IN BRIEF

The department has made improvements to off-site storage, access controls, and physical security since the prior audit. However, control procedures could be improved in the areas of disaster recovery, access controls, program change controls, and monitoring.

RECENT IMPROVEMENTS

Controls over physical access to the building have improved with the installation of a new electronic access system.

The department has improved the security of their off-site storage facility for data back-up, and developed a disaster recovery plan. In addition, the department has recently installed a tracking system that will allow them to monitor and fully document each information system project.

RECOMMENDATIONS

Priority Items

- Improve methods to monitor system security reports and change management reports.
- Implement procedures to document systems project tracking and ensure that only authorized and fully tested software changes are used in production.
- Prohibit program testing in the production environment.

Other Items

- Update the department's disaster recovery plan and perform a full rehearsal.
- Improve internal communications to ensure that employment status changes are reflected in timely changes to computer access.
- Restrict user access to the functions needed to perform the individual's assigned duties.
- Fully document the expected duties and responsibilities of the department's security officer in the job description.
- Set AS/400 security settings to recommended levels.
- Revoke unneeded generic profiles and monitor usage of the remaining ones.

AGENCY RESPONSE

The Department of Revenue generally agrees with the recommendations.

INTRODUCTION

The Department of Revenue (department) is the primary revenue collector for the state of Oregon; with 94 percent of the state's General Fund revenues being collected by the department. The department is responsible for administering and enforcing most of Oregon's tax laws. The primary source of receipts is personal income

tax withholdings; however, the department also collects money for more than 30 smaller programs, including collecting taxes and accounts for other state agencies and some local governments.

The department collected \$4.6 billion from all sources during the fiscal year ending June 30, 1997. Personal income taxes, including withholding taxes, accounted for more than 70 percent of those tax

receipts. All of these receipts were recorded and tracked by the department's information systems. This audit is a follow up of an earlier review of the general controls over these computer systems. It also includes a limited review of the controls over the Personal Income Tax System (PIT) that performs the processing of individual income tax returns. The department processed

1.5 million personal income tax returns for the 1996 tax year.

BACKGROUND

INFORMATION SYSTEMS CONTROLS

Information system controls are typically classified as either general or application controls. General controls are those controls intended to protect the environment in which all applications are processed and do not focus on one specific system. General controls include physical security; access controls; operation controls; back-up and recovery controls; and system design, development, and maintenance controls.

Application controls relate to the specific processing requirements of an individual software application. They are intended to ensure that there are no errors in the recording, classification, and summarizing of authorized transactions. These controls include input, processing, and output controls.

Application control procedures interact with and are complemented by the general computer controls. Because many different applications are processed by the department's computer center, the quality of its general controls has an impact on all the applications processed.

DEPARTMENT OF REVENUE INFORMATION SYSTEMS

The department maintains most of its systems as integrated components, developed in-house over a period of years, operating in the AS/400 environment. Major tax programs, including Personal Income Tax (PIT), Corporation Automated Tax (CAT), and the Integrated Tax Accounting (ITA) systems, have been migrated to the system. Other programs, such as Timber Taxes, are expected to be implemented before the end of the 1997-99 biennium. The department owns two IBM AS/400 computers; it uses one for development, testing, and quality

assurance, the other for production. IBM provides ongoing support for the two computers and the operating system. Routine maintenance on the in-house information systems is the responsibility of the department's employees.

AUDIT RESULTS

Monitoring

The department has established procedures for logging important computer operations and system information. We found several instances, however, in which management could improve monitoring the resulting information.

The department has elected to log authorization failures, object deletions, program failures, save and restore information, and security-related functions. Several of the logs are quite lengthy and include many simple keystroke errors, such as routine mistakes in keying user identifications or passwords. For this reason, management generally only reviews the logs for trends. However, as a result of only monitoring trends, a large number of authorization failures that pointed to an on-going problem were not investigated promptly. Limited monitoring also increases the risk that security breaches may not be detected in a timely manner, and operations may be impaired as a result of unidentified problems.

The department also generates several monthly change management reports, but management does not review them. As a result, the department has an increased risk of unauthorized changes to programs, databases, or files going undetected.

We recommend the department identify the security and change management reports necessary to adequately monitor and manage the department's computer systems. It should then develop procedures to ensure that these reports are monitored.

Agency Response: *We have recently instituted a new procedure. User requests to have their passwords "reset" because they've exceeded the number of tries for a successful sign on are now logged by the operators. The operations staff reviews these logs daily.*

Another recently implemented procedure is to review any object that has been added to or deleted from the system that is greater than one megabyte. We are also monitoring DASD usage for the same one-megabyte increases or decreases. In total, there are six management reports that are reviewed on a weekly basis. This procedure is located in the AS/400 Standards, Policies, and Procedures Manual.

Systems Design, Development, and Modification

The Computer Services Division of the department employs a programming staff to design, develop, and maintain the application programs and database tables used to process the transactions for each tax program.

The department has a Systems Development Life Cycle (SDLC) methodology to ensure that projects, such as changes to existing systems or the development of new systems, are adequately documented and controlled. We found the project documentation was not adequate to determine if the SDLC is being followed. We could not verify that all required approvals or reviews were present for the system update we tested.

When a program is ready to be transferred from the testing region into production, the department requires that the move request include the project number and the programmer's name. The Production Program Administrator then executes the transfer. However, there is no procedure to verify that the transfer request is for a valid project

or that users and management have reviewed the changes and approved the transfer before it is made. As a result, the department risks the potential loss, misuse, or damage to applications, databases, and files from unauthorized, or untested programs being used in production.

We recommend the department produce the documentation necessary to adequately track systems projects and ensure that only authorized, properly tested changes are used in production.

Agency Response: *Our current tracking system contains the status of a task by its tracking number. The record also contains the name of the technician or user who last updated the status. We will modify our current procedure for reviewing the tracking record to indicate that the user has approved, prior to moving the change into production. Two new steps will be added to the Production Program Administrator verification procedure for move requests. First, the Task Tracking Number/Task Number will be checked to verify that the status includes a "User Approved" status. Second, the Task Tracking Number/Task Number list of changed objects will be compared to the objects being moved.*

The move request will not be approved unless the status shows approved by a user and the list of objects to move match the list of changed objects for the task.

Testing in Production Region

The department has created separate environments for testing and production. Separating the test and production regions is a good control technique to assure that only tested, authorized programs are allowed in the production environment. While the system has been designed with this control feature, it is not always being used. Instead, system modification and testing is being performed in both regions. The department's policies

and procedures do not appear to prohibit testing in the production environment. The modification and testing of programs in the production region results in an increased risk of unintentional or unauthorized changes to production databases and files.

We recommend the department prohibit the modification or testing of programs in the production environment. If use of the production environment for changes is necessary due to an emergency situation, the department should institute controls to detect unauthorized changes and ensure that all changes made were appropriate.

Agency Response: *We agree. Our procedure will be updated accordingly and the staff will be trained on the updated procedure.*

Backup and Recovery

Department management has established some appropriate backup and recovery procedures. For example, they maintain weekly systems and applications back-ups at an off-site location to allow recovery in the event of a loss. Currently, the department maintains a month-to-month contract with a vendor for an alternative data processing site and equipment for use should the department's facility become unavailable or inoperable. The department is working with the Department of Administrative Services (DAS) to select a vendor for a long-term contract.

The department also has developed a disaster recovery plan. However, the plan has not been kept current, nor has it been tested. The plan has not been reviewed or revised since its adoption in February 1996. The department has not rehearsed recovery of its systems at the alternate processing site since August 1995. Failure to review, update, and test the plan on a regular basis increases the risk that the department will not be able to

smoothly recover from extended damage to its facilities.

We recommend the department review and update the disaster recovery plan to reflect current conditions. We also recommend the department rehearse the plan as soon as practicable. This would include recovery of all mission-critical processing functions. In the future, responsibility for testing and updating the plan should be assigned to a specific individual who is accountable for performing these steps routinely.

Agency Response: *We agree that we should update the disaster recovery plan, as it applies to the AS/400 environment, with the most current information and will do so. We will schedule a rehearsal whether under our current "hot site" agreement or at the site chosen in the Department of Administrative Services' Request for Proposal process. The rehearsal will be scheduled by July 1, 1998.*

Access

Department management has established a variety of control procedures to assist in restricting access to the system. These include requiring user identification and passwords, establishing group profiles to limit access abilities, and designing a process for setting up and revoking access and monitoring unauthorized access.

These controls do not appear to have been effective in restricting access authority to that needed for current employees to perform their assigned duties. We found that over six percent of the active user identifications were not for current employees. We found a similar problem in the prior audit. We also found authorized users with access authority inappropriate to their responsibilities. This results from not having enough group profiles to differentiate between different types of employees, and from not keeping current on job rotations that change

employees' duties. This was also a prior audit finding. The department is currently working on a project to limit access authority by cost center and job class. This will tie access authority more closely to the duties required by an employee's job description.

As a result of these conditions, the department is at increased risk of data loss, misuse, or damage resulting from unauthorized or inappropriate access.

We recommend department management improve internal communications to ensure that employment status changes are reflected in timely changes to computer access. We also recommend the department continue its project to match more closely access authority to job duties.

Agency Response: *We agree. We have now implemented a new process to inform Computer Services when the status of an employee changes, specifically dealing with seasonal employees (this is where the problem was identified). We are also developing a new computer access form that will assist in identifying terminating employees and those who transfer between cost centers. Further, we are working with our Personnel section to find ways to improve communications between the two sections.*

We are continuing the project of developing a new methodology and procedure to have group or sub-group profiles by cost center. In this way, each group or sub-group will be given access to functions needed to do their specific job. This project is scheduled for completion by June 30, 1999.

Security Officer

The department recruits volunteers from its pool of management service employees to fill the role of security officer. It considers this position to be a developmental opportunity, and

an appointee normally serves for two years. The responsibilities for the security officer are discussed with the appointee, but are not documented as part of a position description.

The responsibility of ensuring the facilities are physically secure may be jeopardized since this function is not assigned as an official part of anyone's job duties. If the duties are not formally included in the job description, it is less likely the performance of these duties will be included in the employee's regular performance evaluations. Also, relying on the oral communication of duties and responsibilities increases the chance that some duties will not be assigned or will be miscommunicated.

We recommend the department include the duties and responsibilities of the security officer in the job description of the individual assigned the job.

Agency Response: *We agree. We will include the duties of the department security officer in that person's position description by July 1, 1998.*

System Settings

The department has selected an array of system security values that coincides with professional literature, with four exceptions.

We recommend the department enhance security by setting the four system security values to the recommended levels.

Agency Response: *Of the four recommended values, we agree with and will implement three. The final one is not practical given our environment. We would be happy to discuss this value with the auditor.*

Generic User Profiles

The department maintains nine generic user profiles. These are individual user profiles that are not assigned to a specific individual, but

are available for use by multiple users. Each has the same level of access as the other individual users in the same group profile. It appears that the department may not need some or all of the generic user profiles. For example, several of these generic user profiles have never been used. Others have the password set so that they cannot be used to sign on to the computer system. In addition, it does not appear that their use is monitored. Managers do not monitor to see if these passwords are used. The system does not track what functions were performed using the generic user ID. Additional access options that extend beyond those necessary for job performance, that duplicate existing access abilities, or that allow users functions other than inquiries increase the risk of loss, misuse, or damage to the data.

We recommend the department revoke all unused or unnecessary generic user profiles. We also recommend that the department monitor the use of the remaining user profiles to ensure that they are only being used by authorized individuals to perform authorized activities.

Agency Response: *We agree. We will determine which ones are needed and document this need. All remaining generic user profiles will be deleted. The manager of the System's Development Unit will monitor all of the PFA On-call requests.*

Improvements Noted

The department, in cooperation with the Department of Administrative Services (DAS), installed an electronic physical access system during our review. Each employee has been issued an electronic badge. This badge allows entry to certain areas of the building depending upon the day, time, and the employee's access level. The system records each access attempt in an electronic log.

The department has provided a secure, environmentally safe off-site storage location for its routine back ups so that software and data are readily available in case they are needed to restore a lost system. The department also has developed a disaster recovery plan.

The programming staff have recently installed a software change management tracking system. If utilized as intended, this system should allow the department to determine the status of all software projects. It will also provide documentation for each project, including management and user approvals and acceptance. It will permit the department to verify that all required steps in the Systems Development Life Cycle procedures have been carried out before transferring the project's programs from a test to production environment.

SCOPE AND METHODOLOGY

The audit encompassed a review of the general controls of the

department's information system, and a review of the application controls of the Personal Income Tax system. This review was performed between August and December 1997. This audit was to follow up on the status of issues and recommendations contained in our previous audit dated April 28, 1995.

The objective of the audit was to determine if the Information Processing Division has developed, documented, and implemented a system of control procedures to provide reasonable assurance of preventing or detecting unauthorized or improper modification or use of its data.

The review included a determination of whether the Information Processing Division had general controls in place to provide for:

- Adequate segregation of duties to minimize the likelihood of errors or irregularities;
- Adequate procedures to monitor the design, development, and

maintenance of computer applications;

- Back-up procedures to protect and recover data in the event of system failure;
- Access controls to prevent unauthorized access to computer hardware, software, and data; and
- Physical security controls that provide reasonable assurance against accidental or malicious destruction or misuse of records and equipment.

The limited application controls review, of the Personal Income Tax system, was designed only to follow up on the findings from our 1995 audit.

We conducted this audit according to generally accepted government auditing standards. We limited our review to the areas specified above.

This report is a public record and is intended for the information of the management of the Department of Revenue, the governor of the state of Oregon, the Oregon Legislative Assembly, and all other interested parties. This report 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 Buffinton-Kelm, CISA, CPA • AUDIT STAFF: Mark Winter, CPA; Nancy Winston, CPA

DEPUTY DIRECTOR: Sharron Walker, CPA, CFE

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

Auditing to Protect the Public Interest and Improve Oregon Government