
Secretary of State

State of Oregon

DEPARTMENT OF REVENUE

Application Controls Review



Audits Division

Secretary of State

State of Oregon

DEPARTMENT OF REVENUE

Application Controls Review



Audits Division

OFFICE OF THE
SECRETARY OF STATE
Bill Bradbury
Secretary of State
Suzanne Townsend
Deputy Secretary of State



AUDITS DIVISION
John Lattimer
Director

(503) 986-2255
FAX (503) 378-6767

Auditing for a Better Oregon

The Honorable John Kitzhaber, M.D.
Governor of Oregon
State Capitol Building
Salem, Oregon 97310

Elizabeth Harchenko, Director
Department of Revenue
955 Center Street NE
Salem, Oregon 97310

This report includes our evaluation of the Department of Revenue's (department) application controls over the Integrated Tax Accounting (ITA) system. During our audit, we reviewed policies and procedures relating to managing system and programming changes; ensuring appropriate data input, processing and output; and providing system security. We also reviewed the status of related recommendations contained in our previous audit of the department's general controls.

The report includes recommendations to improve existing policies and procedures governing the operation, maintenance, and security of the ITA system. Priority items needing attention include developing and enforcing controls over programming changes, physical and logical security, transaction approval and review and control of system outputs. In addition, the department should better account for personal computers, develop an operations manual and further development its disaster recovery and contingency plans.

The Department of Revenue generally agrees with our recommendations.

OREGON AUDITS DIVISION

John N. Lattimer
Director

Fieldwork Completion Date:
November 17, 1999

TABLE OF CONTENTS

	<u>Page</u>
SUMMARY	vii
INTRODUCTION	
BACKGROUND.....	1
INFORMATION SYSTEM CONTROLS.....	1
SCOPE AND METHODOLOGY.....	1
AUDIT RESULTS	
SYSTEM AND PROGRAM CHANGES	3
APPLICATION CONTROLS.....	5
SYSTEM SECURITY	8
OTHER MATTERS	12
PRIOR AUDIT FINDINGS	15
COMMENDATION.....	16
AGENCY'S RESPONSE TO THE AUDIT REPORT.....	17

SUMMARY

BACKGROUND

The Department of Revenue (department) relies on numerous computer applications to administer more than 30 tax programs. These applications interface with the Integrated Tax Accounting (ITA) system that provides common functions such as accounting, check writing, billing and other tax maintenance routines. Using these applications, the department processes about four million documents each year.

AUDIT PURPOSE

The purpose of this audit was to review the application controls governing the ITA system. Application controls relate to the specific processing requirements of individual software applications and are designed to reduce errors that may occur during the operation of the system.

AUDIT RESULTS

The department should consider the following priority items to improve controls governing ITA:

- Update its systems development life cycle (SDLC) methodology to include creation and retention of all supporting documentation, formal approvals, monitoring activities, and system enhancements.
- Further develop its quality assurance plan to ensure adherence to system development standards and procedures.
- Improve control over transaction review and approval, particularly automatic approvals.
- Establish formal procedures to ensure that checks and billings are mailed or diverted appropriately.
- Develop and implement procedures to timely update employee's access to computer systems when a status change occurs.
- Further refine group profiles to ensure that access is adequately specific to the individual's demonstrated need to view, add, change or delete data.
- More effectively communicate and enforce password-reset policies and more closely monitor password-reset logs.

- Further limit programmers' access to the production region to only emergency situations and more closely monitor use of that access.
- Modify the physical security plan to address identified weaknesses and monitor key-card usage.
- Fully develop and maintain its operations manual to include error messages and responses; backup, restart, and restore procedures; and specific requirements to run applications.
- Develop and implement policies and procedures for accounting for computer equipment costing less than \$5,000 including conducting a periodic inventory to verify existence.
- Assign responsibility for fully developing and maintaining disaster recovery and contingency plans.

**AGENCY'S RESPONSE
IN BRIEF**

The Department of Revenue generally agrees with our recommendations.

The department's response to the recommendations begins on page 17. Our recommendations have been numbered to match the department's response.

INTRODUCTION

BACKGROUND

The Department of Revenue (department) administers more than thirty tax programs in addition to the personal income tax. Some of these tax programs include corporate, excise, gift and inheritance, and tobacco taxes. The department processes about 1.4 million income tax returns each year. In all, the department annually processes about four million documents.

To administer these tax programs, the department relies on numerous computer applications. In turn, these applications interface with the Integrated Tax Accounting (ITA) system that provides common functions such as accounting, check writing, billing and other tax maintenance functions. These computer applications reside on the department's central computer system.

The Computer Services section provides for systems development, operations, and network support for these applications. In addition, systems support analysts research system problems, propose solutions, test program changes, and act as liaison between the end users and Computer Services.

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. Application controls relate to specific processing requirements of individual software programs by reducing 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.

SCOPE AND METHODOLOGY

The objective of our audit was to evaluate the adequacy of application controls that the department had in place during our audit period. These controls included policies and procedures to manage system and programming changes; ensure

appropriate data input, processing and output; and to provide system security. We conducted our fieldwork between April and October 1999.

During our audit we interviewed various department personnel, examined documents supporting controls and observed the department's processes and operations. We evaluated compliance with applicable laws, rules, and regulations pertaining to the ITA system. We also reviewed the status of the department's efforts to resolve control weaknesses identified in our last audit report titled *Department of Revenue: General and Personal Income Tax Application Controls*, issued May 7, 1998.

We used the Information Systems Audit and Control Foundation's (ISACF) "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 generally accepted information technology control objectives and audit guidelines. We conducted our audit according to generally accepted government auditing standards.

AUDIT RESULTS

SYSTEM AND PROGRAM CHANGES

The Department of Revenue's (department) Information Processing Department (IPD) is responsible for ensuring that the Integrated Tax Accounting (ITA) system functions to meet user needs and requirements. IPD relies on the Computer Services section and system support analysts to ensure that all user requirements are met and that only authorized changes are made to programs.

Computer programming changes should be made using a written systematic approach that minimizes the likelihood that disruptions, unauthorized alterations, or errors could be introduced into the system. This approach to making programming changes is called System Development Life Cycle (SDLC) methodology. SDLC includes change management procedures for new system development as well as for ongoing system enhancements.

Systems Development

The IPD has an SDLC methodology that outlines major tasks to be performed during system development and specifies the resulting deliverables. 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 including specifications for each program. The IPD, however, only applies this methodology to major project development.

For ongoing system enhancements the IPD uses less formal procedures. For example, many of the defined deliverables are not required. Instead, users submit problem descriptions that include the reason for the requests and user requirements. These requests are approved and prioritized by the Systems Development Planning Committee (SDPC) and then the Systems Development manager assigns them to programmers. When programming is completed, users are to indicate their acceptance of the change. Later, Computer Services requests that users complete a survey to verify that the changes were acceptable.

Computer Services uses an automated task tracking system to document system development progress by identifying major steps completed, tracking who performed the steps and when the steps were completed.

Although IPD has a formal SDLC, its methodology does not include the following important elements:

- Management does not perform a sufficient review of programmer's work to ensure that they only make authorized changes to programs or data.
- IPD's current process for making enhancements to the system does not include necessary elements such as development and approval of testing plans, design specifications or requirements for updating system documentation.

Additionally, IPD has not always followed its SDLC methodology, including the following:

- Computer Services employees said that they did not complete some of the required SDLC deliverables relating to development of the ITA system. They also stated that they threw away important SDLC deliverables including the technical system design and technical procedure development documentation.
- Computer Services also indicated that they threw away the supporting documentation for 47 of the 59 system enhancement requests included in the department's task tracking system. Of the remaining, only 2 were formally approved by the SDPC.
- Users do not always test and approve programming changes before they are made and moved into production.
- Sometimes programmers make programming changes without independent approval or user acceptance.
- Computer Services does not always use the task tracking system to document all major steps that they have completed.
- Computer Services did not always survey users regarding the effectiveness of system changes.

- The department did not always update user manuals and online help screens to reflect changes made to programs.
- The utility program that Computer Services uses to move code into production does not always function as intended.
- Department managers do not always follow established procedures when making changes to tables containing taxpayer notice information.

The above conditions exist because IPD management has not adequately defined and implemented its SDLC methodology. Additionally, it has not developed processes to ensure adherence to system development standards and procedures. As a result, IPD has an increased risk that disruptions, unauthorized alterations and errors could occur.

We recommend IPD:

1. Improve the department's SDLC methodology by including the following additional elements:
 - ❖ Policies requiring creation and retention of supporting documentation for each system change.
 - ❖ Procedures requiring formal approval for each phase of the change process.
 - ❖ Procedures to ensure independent thorough reviews of programmers' work to ensure unauthorized code is not introduced and the programming adheres to standards and expectations.
2. Further develop its quality assurance plan to ensure adherence to SDLC standards and procedures. This approach should prescribe the specific types of activities to be performed, such as reviews, audits and inspections.
3. Consider correcting the utility program used to move code into production or develop compensating controls to mitigate the risk caused by the error.

APPLICATION CONTROLS

Controls Over Data Input

The department relies on various automated routines to provide reasonable assurance that data input errors are detected, reported and corrected prior to processing and that the data is

processed only once. During our review we tested whether selected input routines were functioning as intended. Of these routines tested, we found that ITA properly rejected incomplete or invalid data prior to processing and input control totals did provide assurance that all data input was received for processing.

Controls Over Data Processing

The ITA system has various automated routines to ensure that processing occurs according to current tax laws and department guidelines. For example, ITA has automated routines to ensure that liens are not released until the related tax liability is paid. Therefore, we tested some of these processes to determine if they were operating as intended. For the transactions tested, we concluded the following processes were working properly:

- ITA calculated and applied penalty and interest to taxpayer liabilities at rates allowed by law.
- Refunds were offset only to those programs allowed, and for the correct amount.
- Liens were not released until the liability was either paid in full or the balance was less than the established billable amount.
- Control totals accurately reflected the numbers and amounts of transactions processed through the system.

The following processes were not working as intended:

- Due to a programming error, some refunds processed during fiscal year 1999 did not receive the intended number of reviews and approvals.
- Some employees have been authorized to review and approve transactions even though their position does not include those duties. These reviewers/approvers include Computer Services employees and the internal auditor. In addition, some authorized reviewers are no longer working for the department.
- ITA allows reviewers to award automatic approval of transactions to employees they supervise. However, the department has not effectively maintained this control to

ensure that it continues to function as intended. For example, we found that many of the employees having automatic transaction approval no longer work for the reviewer who granted the automatic approval.

Additionally, we noted that 6 employees in our sample still have automatic approval given to them by reviewers who previously terminated employment at the department.

The above conditions exist because department management has not established sufficient procedures governing who should provide the various levels of transaction review. Additionally, the department does not have procedures to ensure that tables governing reviews are timely maintained. Furthermore, a programming error allows certain transactions to be processed without the intended reviews. These conditions increase the risk that erroneous or fraudulent refunds would not be prevented or detected.

We recommend the department management improve its control over transaction review and approval by implementing the following:

4. 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.
5. Formally assign responsibility to monitor and update the tables governing transaction review and approval to ensure that they remain valid.
6. Remove the review authority awarded to inappropriate reviewers identified during our audit including Computer Services employees and the internal auditor.
7. Correcting 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.

Controls Over Data Output

The department is responsible for establishing procedures to ensure all output from the ITA system is accounted for and distributed to its intended receivers. The department has a special responsibility to ensure that all checks produced through ITA are safeguarded throughout the distribution process.

The Special Services section is responsible for final distribution of ITA output such as refund checks and billings. To ensure that all output is accounted for, ITA notifies the Special Services section of the number of items included in each mailing. During the distribution process some items are intentionally diverted to other department units for further special handling or review.

Although ITA generates transaction counts, the department does not reconcile those counts to the number of items actually mailed or diverted; therefore, the department cannot be sure that all checks or billings generated by ITA were handled properly. Thus, the risk is greater that refund checks or billings could be lost or fraudulently diverted and go undetected. This condition exists because department management has not developed procedures requiring reconciliation of output.

We recommend:

8. The department's management establish formal procedures requiring tracking and reconciliation of ITA output to ensure that all items are appropriately distributed. In addition, we recommend that the internal audit section periodically review those reconciliations to ensure they are effectively performed as intended.

SYSTEM SECURITY

Maintaining User Access

Access to the ITA system should be awarded based on an individual's demonstrated need to view, add, change or delete data. The Operations and Technical Support Unit along with a systems support analyst are responsible for providing access to the ITA system. To facilitate granting access to individuals having the same access needs, the department defined various group profiles to define what resources members of the group may access and what functions they may perform.

We reviewed the access granted to 36 members included in 3 of the 40 group profiles to determine whether their access was appropriately restricted. We found that department management does not always grant access based on employees' demonstrated need to view, add, change or delete data. Seventeen of the 36 members reviewed had access profiles that did not match the employees' assigned duties. Many of these

exceptions occurred when employees transferred to other sections within the department where their access needs were different. In addition, department managers did not sufficiently limit group profiles to ensure employees have access to only those resources needed to perform their duties.

The department has policies and procedures for terminating access rights for employees who resign or otherwise terminate employment. These policies instruct managers to review and update each employee's data access authority when that status changes; however, department managers do not always comply with these policies and procedures. We tested 40 employees who terminated employment between January 1998 and August 1999 to determine whether the department timely revoked their access. Of those tested, 30 were not revoked timely including one who was not revoked until 128 days after she terminated. Additionally, the department did not revoke access for 4 individuals even though their employment terminated from 7 to 18 months prior to our review.

We noted these same control weaknesses during our May 1998 audit of the department's general controls. During our audit, we noted the problem continues to occur. As a result, the department is less able to safeguard information against unauthorized use, disclosure or modification, damage or loss.

We recommend:

9. The department's management ensure procedures are developed and enforced to timely update employees' access when they terminate or their job duties change. Additionally, we recommend that the department refine access group profiles to award access rights based on its employees' demonstrated need to view, add, change, or delete data.

Password Maintenance

The department's Help Desk procedures require that requests for password resets be accepted only from the PC Support staff or the employee's immediate supervisor. This policy is designed to reduce the risk of providing access to sensitive data and programs to unauthorized individuals. In addition, all password resets are to be logged and reviewed daily.

For password resets that occurred between January 1998 and August 1999, we compared the password reset logs to the

system logs to determine whether the department followed the above policies and procedures. Of the resets performed during that time, two-thirds were not adequately documented. Furthermore, Computer Services operators accepted requests for password resets from individuals other than the authorized employees and without adequate verification of the individual's identity. In addition, Computer Services did not perform reviews of the password-reset logs to identify potential problems. These conditions exist because the Operations and Technical Support Unit manager did not adequately communicate and enforce the department's password reset policies.

We recommend:

10. Computer Services management more effectively communicate and enforce its password-reset policies. Computer Services should also log and review all password resets and take appropriate action based on those reviews.

Special Access to Production Libraries

Programmers assigned to perform ITA program changes should not perform other system or user functions. Additionally, programmer access should be restricted to the test region where they perform their work. When emergency changes are required to resolve system problems and enable critical processes to continue, procedures should exist to allow emergency fixes to be performed without compromising the integrity of ITA. This involves the use of special logon-IDs to allow programmers to have temporary access to the production region. This access should be logged and closely monitored. In addition, procedures for emergency fixes should include after-the-fact follow up to ensure that all normal controls are retroactively applied.

The department currently has a special logon-ID allowing programmers to access the production region. Although the department intends this access to be used only to fix bad data that halts production, actual usage includes routine programming functions that should be performed in the program test region. For example, programmers use this access to create and modify menus, change access authorities, access and update master files and conduct tests. Additionally, the Systems Development manager did not ensure that all changes

that programmers made in the production region complied with programming standards and that no unauthorized code was introduced. Furthermore, the programmers' normal access profiles allow them to write, modify or delete data in the production region. Using this access, programmers made modifications to production programs that bypassed the department's program change management procedures. As a result, there is an increased likelihood that disruptions, unauthorized alterations to programs or data, and errors would occur. This condition exists because Computer Services management does not have policies and procedures to monitor and control programmers' emergency access to, and activities performed within, the production region.

We recommend:

11. Computer Services management further limit the programmers' access to the production region. This special access should be granted only to accommodate emergencies. In these special instances, management should closely review the programmers' work to ensure that only authorized changes have occurred.

Physical Access Controls

Department management is responsible for providing physical access controls to protect its computer systems. Physical access should be restricted to only authorized individuals. In 1997, the department installed electronic key-card locks to some doors to limit access within the building.

We noted that several weaknesses exist in the department's controls to limit physical access to its central computer system. These weaknesses include the following:

- Physical access to the Computer Services section, that houses important computer equipment, is not adequately restricted.
- The department's key-card system was not adequately maintained. For example, key-cards were not timely revoked and inventories of key-cards were not conducted on a regular basis. Additionally, key-card access logs were not monitored to identify incidents involving possible unauthorized entry to sensitive areas. Furthermore, the Tax Help section issued key-cards without adequate verification or knowledge of the individual's identity or need for access.

Our recommendations have been numbered to match the agency's response, which begins on page 17.

Some of these conditions exist because the department does not have sufficient policies and procedures governing issuance of temporary key-cards and the physical security plan does not address some potential risks. In addition, department management does not ensure that key-cards are returned according to the policy. Furthermore, the department has not assigned responsibility to routinely monitor key-card logs and usage. As a result, 31 of the 40 terminated staff included in our sample did not have their key-card access deactivated in a timely manner. Of those, one former employee's key-card that provided access to sensitive areas within the building was not deactivated for 445 days.

We recommend:

12. Department management refine and enforce policies and procedures governing issuance of temporary key-cards, and the Physical Security Officer modify the physical security plan to ensure that all sensitive areas are adequately protected. In addition, the Physical Security Officer should routinely monitor key-card logs and usage. We further recommend that the department's internal audit section periodically review physical access controls to ensure the controls remain effective.

OTHER MATTERS

Operations Manual

Computer Services management should ensure that the employees operating ITA have sufficient guidance and direction to perform their tasks. An operations manual should be maintained and should include error messages and responses; backup, restart, and restore procedures; and specific requirements to run the various applications.

Computer Services management has not fully developed an adequate operations manual for the ITA system. Many of their procedures are informal and the department relies on the programmers' knowledge to resolve problems. As a result, applications may not run as intended. For example, we found the operators used an incorrect date when running the annual interest update process. As a result, interest receivable was understated in the department's records as of June 30, 1999 by approximately \$578,000.

We recommend:

13. Computer Services management fully develop their operations manual. This manual should include error messages and responses; backup, restart, and restore procedures; and specific processing requirements.

**Monitoring
Computer Inventory**

The Oregon Accounting Manual requires each agency to ensure that the state's property is accounted for and recommends that each agency identify, record, and control inventory items that have a high risk of loss, such as computer equipment.

The department does not maintain adequate records of computer equipment costing less than \$5,000. Approximately two years ago department management issued a laptop computer to an employee for use at home while attending a class. The laptop was issued without a written agreement. During 1999, the computer was stolen from the employee's home. Current management would have been unaware of the arrangement, except that the employee notified the department after the theft occurred.

Because department management did not have sufficient policies and procedures to account for computer equipment valued at less than \$5,000, they could not provide police with sufficient information such as the model and serial number of the stolen item. Thus, the police could not effectively conduct an investigation or positively identify the computer in the event of recovery.

We recommend:

14. Department management develop and implement policies and procedures to track, safeguard, and control personal use of computer equipment costing less than \$5,000. Further, the department should record and conduct a periodic written inventory of all equipment with higher risk of loss, such as personal computers.

**Disaster Recovery and
Contingency Planning**

Disaster recovery and contingency plans are necessary to ensure that services can be restored in the event of a disruption.

The Computer Services section is responsible for developing and maintaining a disaster recovery plan for the department's computer system. During our 1998 audit of general controls, we noted that the department's disaster recovery plan was not fully developed or tested.

During our current audit, we noted that these conditions continue to exist. Many of the elements required for a successful recovery and continued operations are not current or are missing from the disaster recovery plan. Although Computer Services conducted initial testing, they have not fully resolved issues identified by those tests or scheduled further testing. Furthermore, the department's management has not developed adequate contingency plans. As a result, the department may not be able to fully restore the computer system or continue operations in the event of a disaster. This condition exists because department management has not assigned responsibility for fully developing and maintaining disaster recovery and contingency plans.

We recommend:

15. The department's management assign responsibility for fully developing, maintaining and testing its disaster recovery and contingency plans.

PRIOR AUDIT FINDINGS

This section summarizes the Department of Revenue's efforts to resolve prior audit findings included in our report No. 98-12 titled *Department of Revenue: General and Personal Income Tax Application Controls*, May 7, 1998.

PRIOR AUDIT RECOMMENDATIONS

- | | |
|--|--|
| 1. Identify and monitor the security and change management reports necessary to adequately monitor and manage the departments computer systems. | Partially Resolved. |
| 2. Provide adequate documentation necessary to track systems projects and ensure that only authorized, properly tested changes are used in production. | Unresolved, see pages 3 to 5. |
| 3. Prohibit modification and testing of programs in the production environment and institute controls to detect unauthorized changes and ensure that all changes made are appropriate. | Unresolved, see pages 10 to 11. |
| 4. Review and update the disaster recovery plan to reflect current conditions and rehearse the plan. | Unresolved, see pages 13 to 14. |
| 5. Improve internal communications to ensure timely updating of computer access and more closely match access authority to job duties. | Unresolved, see pages 9 to 10. |
| 6. Document the duties and responsibilities of the security officer. | Resolved. |
| 7. Correct system security values to the recommended levels. | Resolved. |
| 8. Revoke all unused or unnecessary generic user profiles. | Resolved. |

COMMENDATION

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

AUDIT TEAM

Neal Weatherspoon, Audit Administrator, CPA, CISA

Nancy L. Young, CPA, CISA

Virginia Briggs

Paul D. Rainbow

Pam Stroebel, CPA

AGENCY'S RESPONSE TO THE AUDIT REPORT



Oregon

John A. Kitzhaber, M.D., Governor

Department of Revenue

955 Center St NE
Salem OR 97310-2501

May 1, 2000

John N. Lattimer, Director
Secretary of State, Audits Division
255 Capital Street NE, Suite 500
Salem, Oregon 97310

Dear Mr. Lattimer:

This letter and the more detailed statements attached constitute Management's Response to your audit report DEPARTMENT OF REVENUE Application Controls Review.

The DOR management strongly emphasizes ethical conduct, operational excellence, fiscal responsibility, and quality relationships. We believe that the fundamental component of successful organizations and internal controls is the personal character of employees. We know that character is difficult to quantify and measure. However, the tangible and intangible benefits are obvious, over the past several years, DOR has successfully developed and enhanced several major systems in support of our organizational mission.

Two years ago, management recognized renewed emphasis was needed in project management skills to successfully develop and enhance mission critical systems such as ITA. As a result, we invested in project management training for several of our key staff and created a formal project management office. The fundamental methodology of project management parallels our System Development Life Cycle (SDLC) methodology. We are confident that our earlier investment in project management will strengthen and enhance our SDLC.

We recognize the need and have been working to provide a work environment that is safe, secure and conducive to our organizational mission. An example is our decision to install key-card locks in August 1997 to control access to work areas. Previously, these general work areas were accessible to the public during normal work hours. We appreciate your recommendations related to these key-cards and will incorporate them to take full advantage of the key-card system.

Please convey my thanks to your staff for their work and suggestions. I understand and appreciate the control objectives underlying their audit recommendations and will seriously consider these issues as we evaluate our control environment, business needs, and resources.

Sincerely,

Elizabeth Harchenko

Management's Response to Numbered Recommendations

- 1. Management agrees** and will enhance the SDLC methodology through the following actions:
 - Requiring the creation and retention of supporting documentation for each system change. The retention periods will be based on the Archives Divisions General Schedule for Information Management Records.
 - Adding procedures that would require a formal review and approval process when and where appropriate.
 - Implementing a tiered review system for reviewing programming changes made by programmers and analysts and a peer review for programming changes made by senior analysts.
- 2. Management agrees** and will further develop the SDLC quality assurance program by documenting the activities to be performed to help ensure compliance with SDLC standards and procedures. Currently, three system support analysts assigned to the ITA system manager provide considerable quality assurance for ITA. They approve all changes to ITA. They also interface heavily with end users and tax program managers to identify system quality issues. Similar positions provide quality assurance for other major systems such as the Personal Income Tax processing system and the Automated Collections Tracking system (ACT).
- 3. Management agrees with the intent of the recommendation.** However, we understand the inherent limitations of the third party CM utility and it continues to provide an adequate level of functionality and control. Therefore, we will continue to utilize this utility program as we evaluate alternative solutions.
- 4. Management agrees** and will prepare a policy and procedure (PAP) to formally document transaction review and approval policy.
- 5. Management agrees.** We will document procedures to monitor and update transaction review and approval authority.

6. **Management agrees with the intent of the recommendation** and will comply with the PAP developed in 4. above.
7. **Management agrees.** We will correct the programming error. This has been added to the ITA project list.
8. **Management agrees with the intent of the recommendation.** However, we believe that existing compensating controls minimize the identified risks and are more cost effective.
9. **Management agrees** and will reemphasize existing procedures, implement the procedures developed in 5. above, and the Personnel Section will investigate alternative methods of linking employee termination to revocation of access rights.
10. **Management agrees** and will reemphasize existing password-reset policies.
11. **Management agrees with the intent of the recommendation.** We will develop procedures to define appropriate uses of PFA On-Call and implement procedures to monitor compliance.
12. **Management agrees with the intent of the recommendation** and will continue to provide a work environment that is safe, secure and conducive to our organizational mission. Future security enhancements will include increasing the frequency of temporary key-card reconciliations, involving the Agency Security Officer in monitoring physical security (i.e. perimeter controls), and implementing procedures developed in 5. and 9. above.
13. **Management agrees** and will update the computer operations manual.
14. **Management agrees with the intent of the recommendation.** However, the cost of implementing and maintaining a physical inventory of all computer equipment costing less than \$5,000 would exceed the perceived benefit. Therefore, management will limit implementation to laptop computers and other equipment determined by management to be susceptible to theft.

15. Management agrees with the intent of the recommendation. However, management does not believe it is cost beneficial or mission critical to develop and maintain redundant operating systems. Management will reevaluate our initial risk analysis and revised the disaster recovery plan based upon the findings and conclusions from this analysis. The Department's current disaster recovery plan is adequate to ensure that critical systems can be restored in a timely manner. It was recently given a green (go) rating by ProDX as part of the State's Y2K readiness evaluation.

FACTS ABOUT THE SECRETARY OF STATE AUDITS DIVISION

The mission of the Audits Division is to “Protect the Public Interest and Improve Oregon Government.” The Oregon Constitution provides that the Secretary of State shall be, by virtue of his 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.

DIRECTORY OF KEY OFFICIALS

Director

Deputy Director

Deputy Director

John N. Lattimer

Catherine E. Pollino, CGFM

Sharron E. Walker, CPA, CFE



This report, which is a public record, is intended to promote the best possible management of public resources.

If you received a copy of an audit and no longer need it, you may return it to the Audits Division. We maintain an inventory of past audit reports. Your cooperation will help us save on printing costs.

Oregon Audits Division
Public Service Building
Salem, Oregon 97310

503-986-2255

We invite comments on our reports through our Hotline or Internet address.

Hotline: 800-336-8218

Internet: Audits.Hotline@state.or.us

<http://www.sos.state.or.us/audits/auditthp.htm>

Auditing to Protect the Public Interest and Improve Oregon Government