
Secretary of State

State of Oregon

OREGON STATE TREASURY

Evaluation of General Computer Controls



Audits Division

Secretary of State

State of Oregon

OREGON STATE TREASURY

Evaluation of General Computer Controls



Audits Division



Auditing for a Better Oregon

The Honorable John Kitzhaber, M.D.
Governor of Oregon
254 State Capitol
Salem, Oregon 97310-4047

The Honorable Jim Hill
Treasurer of the State of Oregon
State Capitol Building
Salem, Oregon 97310

This report includes our evaluation of the general computer controls in place at the Oregon State Treasury. During our audit, we reviewed policies and procedures relating to systems development, security, backup and recovery of data, contingency planning, and other organizational responsibilities.

The report includes recommendations intended to improve the operation of Treasury's information systems. The recommendations address development of comprehensive Systems Development Life Cycle methodologies and operating procedures, monitoring and testing of environmental controls, maintenance of software records, and disaster recovery and contingency planning.

Because of the sensitive nature of Treasury's business processes, we have issued a separate report outlining our recommendations relating to systems security. This confidential report was prepared in accordance with ORS 192.501 (23), which allows exemption of such information from public disclosure.

The Oregon State Treasury generally agrees with our recommendations.

OREGON AUDITS DIVISION

John N. Lattimer
Director

Fieldwork Completion Date:
November 2, 2000

TABLE OF CONTENTS

	<u>Page</u>
SUMMARY.....	vii
INTRODUCTION.....	1
BACKGROUND.....	1
INFORMATION SYSTEM CONTROLS	1
SCOPE AND METHODOLOGY	2
AUDIT RESULTS	
SYSTEMS DEVELOPMENT.....	3
ENSURING CONTINUOUS SERVICE	5
MANAGING OPERATIONS	6
IT ORGANIZATION AND RELATIONSHIPS	7
ENSURING SYSTEMS SECURITY	8
MANAGING FACILITIES.....	8
SOFTWARE LICENSING AND MONITORING	9
COMMENDATION.....	10
AGENCY’S RESPONSE TO THE AUDIT REPORT	11

SUMMARY

AUDIT PURPOSE

The purpose of this audit was to evaluate Treasury's general computer controls. General controls protect the environment in which software applications process data. These controls relate to systems development methodologies, physical and logical security, backup and recovery of data, contingency planning, and other organizational responsibilities.

BACKGROUND AND INTRODUCTION

The Oregon State Treasury relies on various information systems to provide banking functions for state agencies such as receiving, disbursing and investing funds. It also coordinates the issuance and redemption of the state's bonded debt. In addition, Treasury manages the state's investments under the supervision of the Oregon Investment Council. Treasury relies heavily on its information systems to provide these services.

In April 1999, Treasury's Information Systems Division (IS) completed its migration to a client-server environment. The migration project included replacing most of its critical computer applications as well as some hardware. The new applications included both purchased and internally developed programs.

AUDIT RESULTS

The Oregon State Treasury can improve the general controls governing its information systems in the following areas:

- Further develop and implement comprehensive Systems Development Life Cycle methodologies.

- Update backup procedures, store recovery supplies at the off-site storage facility, and fully develop disaster recovery and contingency plans.
- Fully develop an operations manual including problem escalation procedures and ensure the manual remains up-to-date.
- More closely monitor the work of programmers performing work within the production environment and consider reassigning some duties and responsibilities to better separate critical functions.
- Monitor and periodically test environmental sensors and alarms and periodically train staff in proper use of emergency equipment.
- Formally assign responsibility for maintaining software licensing records and for periodically verifying software use.

AGENCY'S RESPONSE IN BRIEF

The Oregon State Treasury generally agrees with our recommendations.

INTRODUCTION

BACKGROUND

The Oregon State Treasury (Treasury) is the custodian of most of the state's cash and investments. It performs banking functions for state agencies such as receiving and disbursing state funds, and investing cash not immediately required for expenditure. In addition, Treasury manages the state's investments under the supervision of the Oregon Investment Council. It also coordinates the issuance and redemption of the state's bonded debt. Treasury relies heavily on its information systems to provide these services.

Treasury's Information Systems Division (IS) designs, constructs, maintains and enhances information systems and functions. These systems also connect Treasury to its multiple office sites, state agencies, local governments, banks and other financial firms.

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. Treasury's Information Systems Division is responsible for providing an appropriately secure operating environment for these systems.

SCOPE AND METHODOLOGY

The objective of our audit was to evaluate the adequacy of Treasury's general controls. We also evaluated compliance with applicable laws, rules, and regulations pertaining to the operation of information systems. Our audit work included inquiries of Treasury personnel, examination of documents related to controls and procedures, and observation of information systems control processes and operations. We performed our fieldwork between July 2000 and November 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 generally accepted information technology control objectives and audit guidelines.

Because of the sensitive nature of Treasury's business processes, we have issued a separate report that was prepared in accordance with ORS 192.501 (23), which allows exemption of system security information from public disclosure. We conducted our audit according to generally accepted government auditing standards.

AUDIT RESULTS

SYSTEMS DEVELOPMENT

The generally recognized standard for managing the development and maintenance of computer-based systems is to adopt comprehensive System Development Life Cycle (SDLC) methodologies. SDLC methodologies are the policies and techniques used to ensure that all phases of system development and maintenance are adequately addressed.

SDLC methodologies should include a series of steps or phases that have defined goals and target completion dates. The actual phases for each project may vary, depending on whether a system is developed in-house or purchased. System maintenance efforts may not require the same level of detail or phases as new applications; however, the procedures should ensure that many of the same development processes are followed, only on a scale appropriate for the magnitude of the effort. Following structured SDLC methodologies reduces the likelihood that disruptions, unauthorized alterations, or errors could be introduced into the system.

In April 1999, Treasury's Information Systems Division (IS) completed its migration to a client-server environment that included implementation of new hardware as well as system and application software. During the migration, Treasury replaced most of its critical computer applications with programs that were purchased or internally developed. During the system migration, IS did not have fully developed SDLC methodologies to govern its system development. As a result, IS programmers did not adequately document some of their work and did not complete some key system development processes. For example, they generally did not document security considerations or the reviews and approvals of the various phases and occasionally did not document the results of testing. They also did not complete some key deliverables such as development of operating and user manuals or creation of disaster recovery and contingency plans. In addition, IS continues to make enhancements to these systems without adequate SDLC to govern those processes.

Many potential risks arise when adequate SDLC methodologies are not used when making changes to computer-based systems. One important risk is that the end result may not meet the users'

business needs, requirements or expectations. For example, Treasury purchased a limited version of software for a specific project. During initial testing, IS determined that the software would be suitable to meet the intended need. Relying on this assessment, in April 2000, Treasury purchased the full version of the software and a network server for the project. However, during implementation of the software and server, the Systems and Development Supervisor cancelled the project because the configuration was unsuitable for its intended purpose. Because IS did not have formal SDLC methodologies, programmers assigned to the project did not document the tests that supported their recommendations to purchase the software and server. Although IS managers identified an alternate use for the server and intend to use the software for other purposes, as of October 2000, the software was not being used.

Another risk of inadequate SDLC is that unintended code may be introduced into software applications. For example, in September 2000, IS programmers wrote and inserted code into one application to accommodate data format changes. Although IS programmers indicated that they tested the code prior to putting it into production, the code that they actually inserted was not the code that they tested. Thus, when the application was later used, 458 banking transactions did not post to the correct accounts, but rather posted to suspense accounts. To correct these errors, Treasury's banking personnel had to research each transaction error and manually transfer the funds to the correct accounts. IS programmers then fixed the code causing the problem.

Since the migration project, the IS division has been developing SDLC methodologies to govern new application development and changes to their existing systems. However, these methodologies do not address several important system and development maintenance issues. For example, they do not address hardware changes or system and desktop software changes. In addition, they do not adequately address processes for acquiring application software. Furthermore, their SDLC lacks processes to ensure that only intended code will be introduced into the production environment.

We recommend that Treasury management fully develop and implement comprehensive SDLC methodologies. The methodologies should include specific policies and procedures to govern all aspects and phases of the system development life cycle, including the following important elements:

- Procedures governing the changes to hardware as well as system and desktop software.
- Processes for acquiring application software.
- Mechanisms to ensure that only intended changes are introduced into the production environment. These mechanisms may include software to provide for code comparisons.
- Procedures to ensure that all processes are adequately documented and the documentation retained.

ENSURING CONTINUOUS SERVICE

Disaster recovery and contingency planning are necessary to ensure that services can be restored in the event of a disruption. These plans should include procedures to regularly backup information system data and store it in a secure off-site location. They should also provide detailed instruction for recovery from various disaster scenarios. Disaster recovery and contingency plans should be created and tested during system development and put in place during system implementation.

Treasury has developed disaster recovery and contingency plans; however, elements of these plans are incomplete or missing, including the following:

- Various disaster response scenarios from minor to total loss of capability and responses to each, in sufficient detail for step-by-step execution.
- Written agreements to ensure that vendors will provide expected services and that alternate recovery locations will be available and feasible in the event of a disaster.
- Detailed lists of items necessary to recover operations. For example, the plan does not specify necessary supplies and equipment needed at the recovery site; documentation such as operating, system and user manuals; and identification of qualified personnel needed to perform recovery and continue operations.
- Required recovery times and expected system performance norms.

Although Treasury personnel recently conducted testing to restore the computer system at an alternate site out of state, they did not fully document the testing procedures or the results of those tests. In addition, Treasury has not tested the feasibility of using local facilities for recovering day-to-day operations and does not store all the necessary recovery supplies at their off-site storage facility. Furthermore, Treasury's current backup procedures are incomplete. For example, the procedures do not include backup of system files or provisions to ensure the reliability of backup tapes.

These conditions occur because Treasury management did not have a formal SDLC methodology in place requiring development and testing of the plans. Furthermore, Treasury management created the plans with the overall assumption that only the Treasury building would be affected in a disaster. As a result, the risk is greater that Treasury's critical statewide banking functions could be inoperable for a longer period of time in the event of an emergency.

We recommend that Treasury management more fully develop and implement its disaster recovery and contingency plans; ensure that all necessary recovery supplies are stored at the off-site storage facility and update the backup procedures to reflect current systems and practices.

MANAGING OPERATIONS

To ensure that important system functions are performed as prescribed IS management should document standard operating procedures. These procedures should address issues such as error messages and the appropriate responses; backup, restart, and restore procedures; and specific instructions for running the various applications. They also should include problem escalation procedures to identify who should correct specific types of problems and which problems require urgent resolution. Once prepared, the operations manual should be updated on an ongoing basis as applications, systems and hardware change.

During the migration project to the client-server environment, the IS staff did not develop or document the necessary operating and problem escalation procedures. Although operators have begun preparing some basic procedures to guide daily operations, the operating manual remains incomplete. As a

result, problems occurring during processing may not be properly or timely resolved.

We recommend that IS management fully develop an operations manual including problem escalation procedures. Management should periodically review the manual to ensure it remains current.

IT ORGANIZATION AND RELATIONSHIPS

Treasury management is responsible for maintaining an appropriate operating environment for its computer systems. This includes assigning roles and responsibilities to ensure separation of important functions. Separation of duties is important to minimize the likelihood of errors or illegal acts occurring, and to ensure that if such events do occur, they will be detected and corrected timely. Separating programming, database administration and security responsibilities limit the opportunity for a single individual to subvert a critical process. Further, to ensure separation of important functions, programmers should not have access to production databases, application programs or data files.

Treasury's organizational structure does not always support adequate separation of sensitive functions according to best practices. IS managers have assigned programmers to occasionally perform database administration or security functions. Also, IS programmers assigned to individual applications have access to production programs and data. As a result, there is an increased risk that disruptions, unauthorized alterations or errors could occur to programs or data and not be detected timely.

IS management indicated that these conditions exist because the division has limited staff with sufficient expertise to perform these functions. However, IS management does not adequately compensate by strictly monitoring and controlling programmers' access to and activities performed on production programs and data. Mechanisms for monitoring programmers work may include performing code comparisons, logging programmers access to production files, or both.

We recommend that Treasury management consider reassigning programming, database administration and security tasks to provide better separation of these critical functions. We

also recommend IS management more closely monitor the work of programmers performing work within the production environment.

ENSURING SYSTEMS SECURITY

The Oregon State Treasury relies on various manual and automated controls to safeguard information against unauthorized use, disclosure or modification, damage or loss. Because of the sensitive nature of Treasury's business processes, we have issued a separate report outlining our recommendations to improve systems security. This confidential report was prepared in accordance with ORS 192.501 (23), which allows exemption of such information from public disclosure.

MANAGING FACILITIES

IS management should ensure that sufficient measures are in place to protect systems from environmental hazards such as fire, dust, power fluctuations, excessive heat and humidity. Treasury has various mechanisms, such as sensors and alarms, to ensure the safety of both equipment and people against these hazards.

Although mechanisms are in place, Treasury personnel do not monitor environmental controls such as temperature and humidity sensors. Because sensors and alarms are not monitored 24 hours a day, Treasury generally would not be aware of alarms occurring during non-working hours. Additionally, Treasury does not periodically test all alarms and detectors on a regular basis to ensure that they function as intended, nor has it provided periodic training to staff on proper fire extinguisher use. Finally, Treasury management has not fully documented procedures and expected response scenarios for environmental emergencies.

These conditions exist because Treasury management has not developed procedures to ensure alarms and detectors are tested, monitored, and appropriately responded to and the condition resolved. Additionally, Treasury has not provided for remote notification when environmental alarms sound during non-

working hours. As a result, data center staff may be less prepared or delayed in their response to an emergency.

We recommend that Treasury management make the following improvements:

- Develop procedures to monitor and periodically test all sensors and alarms.
- Consider a notification mechanism for alarms occurring during non-working hours.
- Provide periodic training on proper use of fire extinguishers.

SOFTWARE LICENSING AND MONITORING

The IS staff is responsible for ensuring that all software is registered and that users comply with software licensing agreements. To facilitate these tasks, IS has a log to track software installations. However, IS employees do not maintain the log or periodically verify which software is being used on Treasury computers. As a result, Treasury may not be in compliance with software licensing agreements. This condition exists because IS management has not formally assigned the responsibility for maintaining the log or periodically verifying which software resides on Treasury computers.

We recommend that IS management formally assign responsibility for maintaining software licensing records and periodically verifying software use. One possible alternative is to consider purchasing scanning software to better facilitate tracking.

COMMENDATION

The courtesies and cooperation extended by the officials and staff of the Oregon State Treasury during the course of this review were commendable and sincerely appreciated.

AUDIT TEAM

Neal Weatherspoon, Audit Administrator, CPA, CISA

Nancy Young, CPA, CISA

Nancy Winston, CPA, CISA

Jamie Breyman

AGENCY'S RESPONSE TO THE AUDIT REPORT

JIM HILL
STATE TREASURER

GARY H. BRUEBAKER
DEPUTY STATE TREASURER



OREGON STATE TREASURY
350 WINTER STREET NE, SUITE 100
SALEM, OREGON 97310-0840
(503) 378-4000
FAX (503) 378-2870

December 15, 2000

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

Dear Mr. Lattimer

We have reviewed the draft General Controls Review and Confidential Systems Security reports. Our comments to be included in the areas provided in the draft reports are attached.

We appreciate the professional manner in which the audit staff conducted this review and believe the recommendations are very useful to improve Treasury's system security controls.

If you or your staff have any issues or concerns regarding our comments, please call me or Kevin Nordhill at (503) 378-4000.

Sincerely,

Gary Bruebaker
Deputy State Treasurer

GENERAL CONTROLS REVIEW

Treasury generally agrees with the recommendations made in report and have taken the following actions regarding the recommendations where general controls can be improved:

- A comprehensive formal documentation for Systems Development Life Cycle methodologies has been drafted and is in the process of being implemented.
- Treasury continues to be in the process of developing a comprehensive disaster recovery plan which provides for utilization of a hot-site and brings all mission critical systems up within 48 hours. The plan is formally documented and the first two of four phases in testing the plan using the hot-site have been successfully completed.
- A revised operations manual has been drafted and is in use. Formal adoption of the draft procedures will occur shortly.
- Treasury will implement procedures to more closely monitor the work of programmers while updating code in the production environment.
- Treasury will periodically test environmental sensors and alarms and train staff on proper use of emergency equipment.
- Treasury will formally assign the responsibility for maintaining software licensing records and for periodic review of software use.

SYSTEMS DEVELOPMENT

Treasury agrees that the SDLC methodology should be formally adopted. We have drafted a formal SDLC methodology, which includes the four elements recommended in this review, and intend to formally adopt it shortly.

ENSURING CONTINUOUS SERVICE

Treasury has invested substantial human and financial resources revising the disaster recovery plan to be a workable plan. A major revision was necessary due to the recent computer migration. Treasury engaged the services of SunGard Recovery Services in October 1999, embracing their methodology to concentrate only on scenarios that would eliminate all access to and operation of our information system operations. Their thinking in developing the plan was that it is impossible to develop plans for every possible contingency. Planning for only disruptions that eliminate all access to, and operation of our facilities, would allow management to be flexible for multiple scenarios. The focus was to develop responses based upon time away from the building (0 to 48 hours, 3 to 7 days, 8 to 15 days, and 16 to 30 days). Based upon the severity of the disaster, the Incident Management Team would determine a course of action depending upon the estimated time to repair the computer and office spaces.

Treasury has completed two successful tests of the Information Systems section of the Disaster Recovery Plan. The first test, completed in June 2000, was conducted at the hot-site in Scottsdale, Arizona and tested the ability to configure a LAN according to the Disaster Recovery Plan. All test objectives were met and a baseline was determined. A second test at the hot-site was completed in September 2000, repeating the first test, installing and configuring critical applications. While this test was successful, it produced opportunities for improvement. Future tests are currently planned, including a full test of Treasury's communication needs and a final test with users to synchronize systems and input data.

Treasury agrees that the plan is not fully complete until it has been completely tested and that certain elements of the plan can be improved. With that said, Treasury's current disaster recovery plan is significantly improved over any previous plan Treasury has ever had. Treasury will continue to explore documenting procedures to address less disastrous recovery scenarios, which are now handled as day to day operations.

MANAGING FACILITIES

Treasury agrees with the recommendations made and will take the following steps:

- Develop procedures to monitor and periodically test all sensors and alarms,
- Review and evaluate the cost/benefit of a notification mechanism for alarms occurring during non-working hours, and
- Provide periodic training on proper use of fire extinguishers.

SOFTWARE LICENSING & MONITORING

Treasury will formally assign responsibility for maintaining software licensing records and periodically verifying software use.

FACTS ABOUT THE SECRETARY OF STATE AUDITS DIVISION

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

<i>Director</i>	John N. Lattimer
<i>Deputy Director</i>	Catherine E. Pollino, CGFM
<i>Deputy Director</i>	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 report and no longer need it, you may return it to the Audits Division. We maintain an inventory of past audit reports. Your cooperation helps us save on printing costs.

Oregon Audits Division
Public Service Building
255 Capitol Street NE • Suite 500
Salem, Oregon 97310

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

Ph. 503-986-2255
Hotline: 800-336-8218
Internet: Audits.Hotline@state.or.us

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

Auditing to Protect the Public Interest and Improve Oregon Government

