



Secretary of State Audit Report

Department of Administrative Services: Oregon State Payroll Application Computer Controls Review

Summary

BACKGROUND

The Department of Administrative Services (department) provides centralized payroll services to state agencies. The department's State Controller's Division provides centralized accounting and reporting services and is responsible for operation and control of the Oregon State Payroll Application (system).

The system processes payroll for over 36,000 state employees each month. During March 2008, it generated payroll checks and automated deposits totaling approximately \$220 million.

The purpose of this audit was to evaluate the effectiveness of selected general and application computer controls governing the system. Specific audit objectives were to evaluate controls governing data integrity, program modifications, backup and restoration processes, and system security.

RESULTS IN BRIEF

Based on our audit work, we concluded that:

- Application controls provided reasonable assurance that system data, as input by agencies, would remain complete, accurate, and valid.
- System development and change management procedures were adequate, but could be improved to ensure program modifications represent only authorized and approved changes.
- The system and its data were reasonably protected against unauthorized use, disclosure, modification, damage or loss. However, the system was at increased risk of compromise because of security weaknesses at the State Data Center.

- The department did not have assurance that backup tapes were viable or stored off-site.
- Timely or successful restoration of the system in the event of a major disruption would likely be problematic because the department did not have a complete disaster recovery plan, including a written agreement with the State Data Center clarifying disaster recovery roles, responsibilities, requirements or expectations.

RECOMMENDATIONS

We recommend that department management:

- further restrict access to system production libraries and ensure programming code compares are independently performed and evaluated;
- ensure the recommendations we included in the State Data Center confidential security report are timely implemented;
- ensure that backup tapes are viable and stored off-site; and
- develop and test a comprehensive disaster recovery plan to ensure timely restoration of the system in the event of a major disruption, including a written service level agreement with the State Data Center clarifying each division's disaster recovery roles, responsibilities, and expectations.

AGENCY'S RESPONSE

The Department of Administrative Services generally agrees with the recommendations.

Background

The Department of Administrative Services (department) provides centralized services to state agencies. The department's State Controller's Division provides statewide accounting and reporting services and is responsible for the state's enterprise payroll application.

The Oregon State Payroll Application (system) processes payroll for over 36,000 state employees each month. During March 2008, the system generated payroll checks and automated deposits totaling approximately \$220 million.

During processing, the system receives employee and salary information from the Position and Personnel Database application (PPDB) and provides financial inputs to the Statewide Financial Management Application (SFMA).

The Enterprise Application Services (EAS) section within the department's Operations Division is responsible for system programming code modifications. The system is currently hosted at the department's State Data Center.

Purpose

The purpose of this audit was to evaluate the effectiveness of key general and application computer controls governing the system.

General controls are embedded in information technology processes. They are designed to protect the environment in which all software applications operate. Examples of general controls include system development methodologies, program change management procedures, security, and backup routines.

Application controls are embedded in business processes. They are application specific controls designed to enforce

internal controls or ensure system information remains complete, accurate and valid.

Specific audit objectives were to evaluate controls governing data integrity, program modifications, backup and restoration processes, and system security.

Audit Results

Application Controls Reasonably Ensured OSPA Data Integrity

Effective application controls include both manual and automated processes to ensure only complete, accurate, and valid information is entered into a computer system; data integrity is maintained during processing; and system outputs conform to anticipated results.

We found that manual and automated application controls governing the system were well documented. In addition, the department had detailed written procedures to guide staff and system users regarding control processes.

To verify controls were working as intended, we also performed various tests of application controls governing error detection, data correction, and interfaces with PPDB and SFMA. We also tested selected data files to ensure they included necessary data elements and conformed to established formats.

Based on the results of these tests, we concluded application controls provided reasonable assurance that system data, as input by agencies, would remain complete, accurate, and valid.

System Development and Change Management Procedures were Adequate But Could Be Improved

Management should ensure that all changes to computer applications are appropriately authorized, documented, tested, and approved. Proper change management processes should also ensure that only approved program modifications are implemented.

Employees of the Oregon State Payroll Services (OSPS) section of the State Controller's Division are responsible for managing the system, including approving, testing, and implementing program modifications. The department's Enterprise Application Services (EAS) staff make programming code changes as directed by OSPS.

We evaluated the department's system development and program change management procedures for the system. Based on those tests, we concluded that the department's procedures were sufficient and effective to ensure system modification requests were appropriately prioritized, authorized, assigned, documented, and tracked by EAS and SFMS staff.

However, we noted two related weaknesses in the department's procedures for testing and elevating code to production. First, all EAS staff making system programming changes had access to the acceptance and production code libraries, and could potentially modify code after it was tested and approved. Second, automated code compares were sometimes performed by the same programmer that made the changes.

As a result, department managers did not have complete assurance that all program modifications represented authorized and approved changes. While we concluded that controls in place at

user agencies could detect such transactions, we believe the department should address these weaknesses because they increase the risk that programmers could introduce unintended or fraudulent transactions.

We recommend that department management further restrict access to the system production libraries and ensure programming code compares are independently performed and evaluated.

Agency's Response:

We agree with this recommendation. The Department's Operations Enterprise Application Services (EAS) will immediately implement a semi-independent code compare review to be performed by staff from the Open Systems unit of EAS. Each review performed will be documented and approved with signatures. EAS will also implement changes to the OSPA acceptance region that will exclude the OSPA developers from accessing the code. This will eliminate the possibility of unauthorized changes to the region.

EAS is presently considering the cost-benefit of software designed to monitor and track changes made to the production libraries. This software would create an audit report documenting change activity.

**Logical Access Controls
Were Adequate But Data
Center Weaknesses
Pose Risks**

Executive management is responsible for establishing an overall approach to security and internal control that ensures the integrity of computer systems and other information assets. Effective security should follow a layered approach that protects the environment in which systems operate and include logical access

controls to ensure system assets are further protected against unauthorized use, disclosure, modification, damage or loss.

Logical access to computer applications should be restricted according to each user's individual need to view, add or alter information. In order to maintain this principle of "least-privilege," organizations should have formal processes for timely granting, issuing, suspending and closing user accounts. In addition, management should periodically review and confirm users' access rights to ensure that they remain appropriate.

We noted that logical access to system screens was primarily controlled through program code that limited access to data and resources based on information stored in user account profiles. Accordingly, we evaluated the department's processes for granting and managing user accounts. In addition, we tested user profiles to determine whether they conformed to the department's internal control policies. We also tested other logical access mechanisms designed to protect system files and data from access not initiated through the application. We found that these controls were operating as intended and provided a vital layer of security to protect the system against unauthorized use, disclosure, modification, damage or loss.

However, on August 6, 2008, we issued a separate confidential audit report (2008-CS1) to communicate the results of security work we performed during a separate audit of the State Data Center, which hosts the system. In that report, we identified specific security weaknesses relating to the computing environment provided by the data center.

Based on these results, we concluded that the system and its data were reasonably protected

against unauthorized use, disclosure, modification, damage or loss. However, the system was at increased risk of compromise because of security weaknesses at the data center.

We recommend that the department ensure the recommendations we included in the State Data Center confidential security report are timely implemented.

Agency's Response:

As stated in our response to your State Data Center (SDC) confidential security report No. 2008-CS1 dated August 6, 2008, management believes security may be further enhanced through careful considerations of the review's findings and recommendations. We will continue to work toward progress on these issues as specifically addressed in that document.

**Disaster Recovery
Strategies Were Incomplete**

Organizations should ensure that usable backups are regularly performed in accordance with a defined back-up strategy. This strategy should ensure all critical files are copied as frequently as needed to meet business requirements. System disaster recovery procedures should also be well documented and tested to ensure proper and timely restoration of the system in the event of a major disruption.

Department staff ensured weekly backup tapes of critical system files were created at the State Data Center. However, they did not have assurance that backup tapes were viable or were stored off-site. The department also did not have adequate procedures for restoring the system in the event of a major disruption. In addition, the State Controllers Division did not have a written service level agreement with the State Data Center to

clarify disaster recovery roles, responsibilities, and requirements.

As a result, we concluded that successfully restoring the system in a timely manner would likely be problematic.

We recommend that the department obtain assurance that backup tapes are viable and stored off-site.

Agency's Response:

On July 28, 2008 the SDC Advisory Board approved a written service catalog. This service catalog included defined roles and responsibilities that were agreed upon by the SDC and agency participants. The sections of the service catalog that address these specific concerns are 1. SDC Storage Services, 2. Storage and Space Management, 3. Backup, Restore, and Recovery and 4. Continuity and Recovery Management.

The department, as a customer of the data center, will develop a service level agreement relating to the services the data center provides (as outlined by the service catalog). This SLA will outline appropriate protocols for the various program/division application and services that reside at the data center so expectations are defined and followed.

We also recommend that the department develop and test a comprehensive disaster recovery plan to ensure timely restoration of the system in the event of a major disruption. The plan should include a written service level agreement with the State Data Center clarifying each division's disaster recovery roles, responsibilities, and expectations.

Agency's Response:

We agree with this recommendation. The State Controller's Division (SCD) has outlined internal procedures for Disaster Recovery. Both EAS and

SDC have indicated that they have disaster recovery procedures. The procedures and processes have not been tested and SCD will work with EAS and SDC to perform a testing of the defined procedures. As addressed in our response to the third finding the SDC has created a service catalog that addresses continuity and recovery management.

Objectives, Scope and Methodology

The objectives of this audit were to determine whether controls over the system provide reasonable assurance of the following:

- Data remains complete, accurate, and valid during system input, processing, and output.
- Program modifications follow approved system development processes and change management procedures.
- The system and data are reasonably protected against unauthorized use, disclosure, modification, damage, or loss.
- Backup and restoration procedures have been implemented to ensure system services will be available as required in the event of a major disruption.

To test application controls, we evaluated error detection and correction routines, and the system's interfaces with the Personnel and Position Data Base application (PPDB) and the Statewide Financial Management Application (SFMA). In addition, we performed various electronic integrity tests of March 2008 system data.

We tested program change management controls by evaluating related policies and procedures, system file metadata, and

documentation relating to selected program modifications.

To determine whether the system and its data were reasonably secure, we reviewed and evaluated department security policies and procedures, logical access to system files, and logical access controls provided through the application.

For backup and recovery objectives, we reviewed the process for creating backups, and evaluated the department's backup and recovery procedures and plans.

We used the IT Governance Institute's (ITGI) publication, "Control Objectives for Information and Related Technology," (COBIT) to identify generally accepted and applicable internal control objectives and practices for information systems.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.



**Secretary of State
Audits Division**

**255 Capitol St. NE, Suite 500
Salem, OR 97310**

**Auditing to Protect the
Public Interest and Improve
Oregon Government**

AUDIT MANAGER: *Neal E. Weatherspoon, CPA, CISA, CISSP*

AUDIT STAFF: *Mark A. Winter, CPA, CISA
Sarah A. Anderson
Jason A. Butler*

DEPUTY STATE AUDITOR: *William K. Garber, CGFM, MPA*

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

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

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

by phone at 503-986-2255

or by mail from:

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