



Secretary of State Audit Report

Oregon Public Employees Retirement System: jClarety Application Controls Review

Summary

PURPOSE

The purpose of our audit was to evaluate the effectiveness of key general and application computer controls relating to the Oregon Public Employees Retirement System's (PERS) current implementation of the jClarety computer application (application). Our specific audit objectives were to determine whether PERS had implemented controls to reasonably ensure data integrity, system security, program change management, and system backup and recovery.

RESULTS IN BRIEF

Based on our audit work we found that:

- Modifications to jClarety program code followed approved change management procedures.
- Application controls provided reasonable assurance that valid information entered into the system would remain complete and accurate during processing and output. However, those controls did not effectively prevent or detect some data errors.
- Adjusting entries made by PERS staff were not always reviewed, approved or validated, increasing the likelihood that inappropriate data transactions or errors could be introduced into the system.
- The agency's security framework did not adequately protect the application and its data. Because of their sensitive nature, we issued a separate report detailing our security findings and recommendations. ORS 192.501 (23) exempts such information from public disclosure.
- Agency procedures did not ensure all system files and data were appropriately backed up to facilitate timely restoration.

RECOMMENDATIONS

We recommend that PERS management take appropriate action to:

- Resolve data anomalies identified during the audit and implement automated or manual controls to prevent similar instances from occurring, or detect and correct them should they occur.
- Develop and implement formal procedures to ensure that all adjusting entries made by PERS employees are independently reviewed, approved, validated, and documented. Employers should also be notified of any changes made to their members' accounts by PERS employees.
- Implement recommendations included in our confidential security report.
- Revise and further develop backup strategies and resolve the technical issues limiting the agency's ability to execute regular and complete backups.

AGENCY'S RESPONSE

PERS management agrees with the audit findings and has taken action to implement the audit recommendations. PERS' complete response is included on page 6 of this report.

Background

The Oregon Public Employees Retirement System (PERS) provides retirement programs for approximately 881 separate public entities including Oregon state agencies, cities and counties, school districts, and other qualifying public corporations. During the 2006 fiscal year, PERS maintained retirement programs for approximately 315,000 individuals, including more than 101,000 retired members receiving benefits. Net Assets held in trust by PERS to pay future benefits exceeded \$56 billion as of June 30, 2006.

In 2003, the Oregon Legislature passed law to revise existing PERS Tier I and II retirement programs and to create a new program, the Oregon Public Service Retirement Plan (OPSRP). OPSRP consists of an Individual Account Program (IAP) coupled with a defined benefit package. Changes to Tier I and II retirement programs included the addition of IAP accounts and altered how subsequent member contributions would be applied to existing member balances. These changes applied to new members hired on or after August 29, 2003, and for existing Tier I and II members on January 1, 2004.

PERS staff uses the agency's Retirement Information Management System (RIMS) to manage Tier I and II retirement accounts. However, because of known problems with RIMS and the additional requirements imposed by the above pension reform, PERS management obtained legislative approval to replace RIMS with a computer application that could better meet its business needs.

In September 2003, PERS contracted with Covansys Corporation to install and customize the company's jClarety computer system. Implementation

of jClarety is a multi-year project scheduled for completion in 2010. PERS management indicated the OPSRP phase of this project was completed during December 2006. However, functionality for processing member and employer contributions, including IAP contributions, was in place in June 2005. At the time of this audit, PERS staff continued to use RIMS to compute retirements, process payments and maintain certain Tier I and II retirement accounts.

PERS management has primary responsibility for ensuring the availability, confidentiality and integrity of retirement plan records it keeps on computer systems. However, PERS staff must rely on participating employers and plan members to provide valid and complete information in order to achieve these objectives. In that regard, PERS shares the responsibility for ensuring the accuracy and validity of jClarety data with these external partners.

Prior to jClarety, plan information was input and corrected by PERS staff. With the advent of jClarety, employers' staff now perform these functions from their external locations via an internet interface (EDX). PERS staff indicated that employers submit approximately 230,000 member records monthly through the EDX system.

Audit Objectives and Scope

The purpose of our audit was to evaluate the effectiveness of key general and application computer controls relating to the implemented portions of the Oregon Public Employees Retirement System's (PERS) jClarety computer application (application).

Our specific audit objectives were to determine whether PERS had implemented controls to provide reasonable assurance that:

- data input into the application were complete, accurate and valid, and remained so during system processing and output;
- the application and its data were reasonably protected from unauthorized use, disclosure, modification, damage, or loss;
- system files and data were appropriately backed up and could be timely restored; and
- modifications to the application followed approved change management procedures.

Audit Results

Application Controls Should Be Strengthened To Improve 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.

During our audit, we performed various tests of jClarety data to determine the effectiveness of manual and automated application controls. Based on the results of this work, we concluded that application controls provided reasonable assurance that valid information entered into the system would remain complete and accurate during processing and output. However, controls to prevent, detect, and correct invalid data input should be strengthened to better ensure integrity of some jClarety data elements.

Specifically, application controls provided reasonable assurance that the system could properly:

- compute employer and member contribution amounts;
- calculate billings to employers and track corresponding account receivables;

- update accounting records;
- process member IAP account amounts; and
- ensure required data transmissions to the third-party IAP administrator, CitiStreet.

However, application controls did not effectively prevent or detect some data errors. In addition, adjusting entries made by PERS staff were not always reviewed, approved, or validated.

Application Controls Did Not Effectively Prevent or Detect Some Data Errors

Transaction data should be subject to a variety of controls to check for accuracy, completeness and validity. These application controls should be in place for system-generated and interfaced inputs as well as those occurring from manual inputs.

Application controls built into jClarety perform various checks for data validity. These checks were designed to either prevent inappropriate information from being entered into the system or detect it during processing cycles. The four automated checks we tested were working as intended. During May 2006 more than 100,000 data transactions were identified and suspended by automated system edits so that they could be corrected.

However, tests of data identified two situations where application controls should be strengthened to provide better assurance of data integrity. Those situations involved coding for qualified wages and postings of hours worked.

Data transaction records used to report qualifying wages are to contain a specific identifying "wage" code. This code signals the system to compute the associated employer and employee contribution amounts using the

various qualifying wage fields. When only non-qualifying monies are paid to employees, data transaction records are to contain a specific wage code and no contributions are computed.

For the period we tested, more than 23,000 records had wage codes signifying they contained qualifying wages, but no qualifying wages were included. Rather, those data transactions had amounts included in non-qualifying wage fields. We concluded that these contradictions significantly clouded the intent of the data transactions. As a result, PERS staff could not be certain whether amounts were entered into the wrong wage field, or whether erroneous identifying codes were applied to the data transactions. As a worst case, an amount posted to the wrong wage field would be inappropriately excluded from the contribution calculation and associated postings to employer and member accounts.

The system also tracks hours worked by members in order to determine their eligibility. Therefore, it is critical that the underlying data be accurate. During our audit, we analyzed the data fields containing regular and overtime hours worked. For the period tested, there were more than 5,200 member records that reported hours in excess of the 250 that we concluded would be reasonable for a single pay period. These included 51 member records with more than 1,000 reported hours.

We concluded that the greatest impact of data errors relating to hours worked would likely be isolated to new employees or members who do not regularly work full-time. For members in these categories, inaccurate reporting may result in inappropriate eligibility determinations affecting amounts owed by employers and contributions applied to member accounts.

We recommend that PERS management take appropriate action to resolve the above identified data anomalies. We also recommend that management implement automated or manual controls that will either prevent such instances from occurring or timely detect and correct them should they occur.

Adjusting Entries Made By PERS Staff Were Not Always Reviewed, Approved, or Validated

Organizations should establish procedures for correcting data which was erroneously input. Those controls should ensure that adjusting entries are accurate, valid, and independently approved. To maintain appropriate separation of duties required for good internal control, data corrections should generally be performed by those responsible for original input and approved by someone independent of data entry. When data corrections are performed by other staff, procedures should be in place to ensure that an appropriate level of internal control is maintained.

Employers' staff had primary responsibility for entering member data into jClarety and for resolving data errors that occur during input. However, employers often requested that PERS staff input certain entries or make adjustments on their behalf. At the time of our audit, PERS had approximately 35 fulltime equivalent positions assigned to this task.

Although 18 of the 35 staff members were assigned to specific employers' accounts, the entire group could input new entries or adjustments to any member account, including their own. In addition, with few exceptions, the system did not require entries made by staff to be independently reviewed or authorized.

These weaknesses increased the likelihood that inappropriate transactions or erroneous information could be introduced into the system.

We concluded that these control issues existed because PERS management had not implemented sufficient manual controls to compensate for those not provided through the system. We specifically noted that PERS management had not assigned the responsibility for monitoring, validating, documenting, approving and notifying employers of adjustments made to member accounts.

We recommend that PERS management develop and implement formal procedures to ensure that all adjusting entries made by their employees on behalf of employers are independently reviewed, approved, validated, and documented. Those procedures should also ensure that employers are specifically notified of any changes made to their member's accounts by PERS employees.

Security of System Data and Programs Should Be Improved

Executive management is responsible for establishing an overall approach to security and internal control to ensure protection of resources and to maintain integrity of computer systems.

We concluded that PERS' security framework did not adequately protect the application and its data from unauthorized use, disclosure, modification, damage, or loss.

Because of the sensitive nature of system security, we have issued a separate report outlining specific details of our findings, as well as recommendations to improve security. That confidential report was prepared in accordance with ORS 192.501 (23), which exempts

such information from public disclosure.

We recommend that PERS management implement the recommendations included in our confidential report.

Backup and Restoration Strategies Were Inadequate

Organizations should ensure that usable backups are regularly performed in accordance with a defined back-up strategy. Those strategies should ensure all critical files are copied as frequently as needed to meet business requirements. They should also ensure that backup media is securely stored at both on-site and off-site locations. In addition, restoration procedures should be well documented to facilitate the proper and timely recovery of files from backup media.

The agency's backup strategies did not provide adequate assurance that all system files and data were appropriately backed up to facilitate timely restoration. Significant weakness in those strategies included the following:

- Automated backup software could not properly process files that were routinely open during scheduled back-ups.
- One firewall was configured to prohibit back-up server access to servers running in the network's Demilitarized Zone (DMZ).
- Backup error logs were not effectively reviewed to identify what, if any, critical files had been missed during routine backup jobs.
- Backup and restoration policies and procedures were predominately informal and undocumented.

As a result of the above, information residing on certain file servers was not routinely backed

up. In addition, files that were in an open state during routine backup jobs were similarly excluded. Because backup tapes represented an incomplete subset of relevant files and records, files recovered from tape may not actually represent the anticipated state of those files. As a consequence, PERS was less likely to be able to timely, or fully, recover from an interruption.

We concluded that the above technical deficiencies likely occurred as a result of PERS' informal and undocumented approach to providing backup and restoration services.

We recommend that PERS management revise and further develop formal backup strategies, and correct technical barriers limiting the agency's ability to execute regular and complete backups. Those efforts should specifically ensure that back-up software is appropriately configured, and has the required functionality, to fully carry out backup strategies. Efforts should also include development of detailed procedures for restoring the system from backup tape and for providing regular and effective monitoring of backup processes.

Modifications to jClarety Followed Approved Change Management Procedures

Management should ensure that all changes to computer systems follow formal change management procedures. Those procedures should ensure that all system modifications have been appropriately prioritized, authorized, thoroughly tested, and approved prior to being placed in production.

During our audit, we evaluated the change management procedures PERS staff used to control jClarety program modifications. Those procedures required structured

reviews of all change requests, prioritization of proposed modifications, thorough testing of program changes, and formal user approval prior to final implementation.

For the program modifications we tested, PERS staff followed the agency's established change management policies and procedures. We observed that staff followed the prescribed initiation, approval, and prioritization processes. In addition, they thoroughly tested the program changes before approving them and placing the code in production. Actual code modifications were performed by third-party contractors who were responsible for providing version control over the code prior to delivering it to PERS for testing and final approval.

Based on the above, we concluded that jClarety program modifications followed approved change management procedure, which minimized the likelihood of disruption or unauthorized alterations.

Agency's Response:

PERS management agrees with the audit findings and has taken action to implement the audit recommendations. PERS' complete response is included on page 6 of this report.

Audit Methodology

During our audit, we interviewed department personnel and contractors assigned to jClarety (application). In addition, we examined technical documentation relating to the application and its architecture, including documentation regarding networks controlled by PERS. We performed fieldwork between May and October 2006.

To evaluate system application controls we used standard data query tools to perform various electronic tests designed to:

- determine the validity and reasonableness of certain member demographic data;
- compare data submitted by employers to amounts posted to the system;
- validate employer contributions and billings computed by the system;
- verify system calculated receivable amounts; and
- validate system output files directed to CitiStreet, the IAP administrator, and to the Statewide Financial Management Application (SFMA).

To determine whether the application and its data were reasonably secure, we reviewed PERS security policies and procedures, evaluated logical access controls, tested physical access to critical computing resources, and evaluated critical network perimeter security components controlled by PERS.

To test program change management controls, we first evaluated PERS' change management policies and procedures. We then examined applicable documentation supporting the review and approval processes for a recent major software release.

We tested backup and restoration controls by reviewing backup system log entries, backup procedures, and by confirming the existence of off-site storage.

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 our audit according to generally accepted government auditing standards. We also conducted our audit according to Information Systems Audit and Control Association standards for information systems auditing.

Oregon Public Employees Retirement System's Response to the Audit Report

No. 1 – We recommend that PERS management take appropriate action to resolve the above identified anomalies. We also recommend that management implement automated or manual controls that will either prevent such instances from occurring or timely detect and correct them should they occur.

Agency's Response: **Agree**

PERS has identified problems with employer reporting using incorrect or inconsistent coding for non-qualifying wages, non-subject salary and hours worked. The Agency is using a combination of controls in jClarety and other compensating control mechanisms to ensure accuracy, completeness and validity of the data.

PERS identified earlier that many of the excess reported hours were due to a small number of employers with programming issues. These employer-specific programs have since been fixed, but a retroactive clean up is necessary by the affected employers. Additionally, our system flags the employer for any unposted records in excess of 200 hours for the pay period. The flag alerts the employer to a problem with the number of reported hours, but the record still posts.

To address these problems and other data validation and accuracy concerns, PERS is implementing a variety of techniques to control, prevent, detect and correct data in the jClarety system. Specifically,

1. PERS is instituting a post-Annuals clean up process with the employers to include amendment of records needed to complete, validate, and verify the accuracy of yearly data, including qualified wages and hours. This process will address the issues identified by the Audit Report. Anticipated Completion Date: June 2007.
2. PERS is strengthening its employer education and outreach program. During 2006, PERS staff conducted 19 Employer Outreach presentations to address problems of incorrect data reporting. This outreach provided training to over 400 payroll staff representing more than 250 employers. Similar sessions will be conducted in 2007. Anticipated Completion Date: Ongoing.
3. PERS continues to assist employers by issuing guidance on system and data reporting changes as well as expanding hands-on user training to incorporate data quality and validity issues. During 2006, PERS provided guidance relating to EDX Release 4.1 and trained 120 employer representatives in the correct data entry procedures. Additional guidance and training will be provided to employers in 2007. Anticipated Completion Date: Ongoing.
4. PERS is incorporating exception reports in the Data Mart/Warehouse Project to identify potential data errors that compromise our system. In addition, PERS is creating control mechanisms that alert employers to data anomalies that need to be addressed. Anticipated Completion Date: April 2008.
5. PERS is verifying data at critical trigger events throughout a member's career, (e.g. annual member statements), and will be expanding those efforts as part of ongoing operations. Moreover, before a benefit distribution is made, the member's account is reviewed and employers are required to correct erroneous member data and pay any outstanding contributions and accrued earnings associated with the corrected data. Anticipated Completion Date: Ongoing.

No. 2 – We recommend that PERS management develop and implement formal procedures to ensure that all adjusting entries made by their employees on behalf of employers are independently reviewed, approved, validated, and documented. Those procedures should also ensure that employers are specifically notified of any changes made to their members' accounts by PERS employees.

Agency's Response: **Agree**

In November 2006, PERS wrote and implemented new procedures for PERS staff that adjust entries to members' data in jClarety. Specifically the procedures:

1. Notify the employer of any changes made by PERS staff to their member accounts.
2. Request the employer to independently review, approve and validate the changes.
3. Require staff to enter notes into jClarety indicating the reason for the change that was made.
4. Require employer-generated requests to be filed in the employer-specific file for easy reference.

No. 3 – We recommend that PERS management implement the recommendations included in our confidential report.

Agency's Response: **Agree**

PERS agrees with the confidential security report and will be implementing the recommendations.

No. 4 – We recommend that PERS management revise and further develop formal backup strategies, and correct technical barriers limiting the agency's ability to execute regular and complete backups. Those efforts should specifically ensure that back-up software is appropriately configured and has the required functionality, to fully carry out backup strategies. Efforts should also include development of detailed procedures for restoring the system from backup tape and for providing regular and effective monitoring of backup processes.

Agency's Response: Agree

PERS Technical Operations Section (TOS) staff worked with Secretary of State auditors throughout the audit period and made adjustments based on auditor recommendations during the audit. Some of the recommendations have already been implemented and others are planned. The following is a status of the recommendations:

- 1. An upgrade planned during the first quarter of 2007 to the current backup software will allow staff to backup open files and encrypt data stored on tapes.*
- 2. The firewall was reconfigured in August 2006 to allow regularly scheduled backups on the DMZ.*
- 3. Backup logs are now reviewed on a daily basis and previous night's backup issues are identified and resolved during the workday and files are backed up on the next regular schedule.*
- 4. Policies and procedures are being reviewed and will be updated during the first quarter of 2007.*

During the course of the 2007-2009 biennium, TOS will work with the various business units to develop service levels to identify all critical data and ensure that it is backed up according to business needs and can be recovered according to defined service level agreements.



**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
Todd D. Kimball, CPA*

DEPUTY DIRECTOR: *Will K. Garber, CGFM, MPA*

The courtesies and cooperation extended by the officials and staff of the Public Employees Retirement System 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/audithp.htm>

by phone at 503-986-2255

or by mail from:

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