
Secretary of State

State of Oregon

PUBLIC EMPLOYEES RETIREMENT SYSTEM
Information Technology Application Control Review



Audits Division

Secretary of State

State of Oregon

PUBLIC EMPLOYEES RETIREMENT SYSTEM
Information Technology Application Control 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

The Board of Trustees
Oregon Public Employees Retirement System
11410 SW 68th Parkway
Tigard, Oregon 97223

This report presents our evaluation of computer controls governing the Retirement Information Management System (RIMS), Benefit Calculation Sub-System (BCSS) and its associated work-arounds. RIMS supports PERS core business function by accounting for retirement transactions. Within RIMS, the BCSS calculates member benefit amounts and the related adjustments to various reserve accounts.

Currently, PERS is involved in a project to replace the RIMS system and its associated work-arounds. Based on our evaluation of the agency's processes governing system development and maintenance, we conclude that the business risks associated with this project may be significant. Those risks include an increased likelihood that the new system may not include all the necessary elements to meet user needs, provide adequate control or allow for effective future modifications. Additionally, the risk is greater that PERS will not be able to adequately maintain the new system, once implemented.

Our report recommends that PERS implement a more comprehensive system development life cycle (SDLC) methodology before proceeding further with its development plans. We also recommend that PERS mitigate the risks associated with the existing inadequacies of RIMS and improve system security.

During the audit, we became aware of other issues relating to PERS operations. Related to these issues, we make recommendations for PERS to change the benefit calculation

methodology for addressing certain lump sum retirement calculations, enforce its purchasing rules, and improve management of accounts receivable.

OREGON AUDITS DIVISION

John N. Lattimer
Director

Fieldwork Completion Date:
March 23, 2000

TABLE OF CONTENTS

	<u>Page</u>
SUMMARY	vii
INTRODUCTION.....	1
CHAPTER I: SYSTEM DEVELOPMENT AND MAINTENANCE.....	5
SDLC METHODOLOGY	5
EFFECTS OF INCOMPLETE SDLC.....	7
Testing Standards and Requirements.....	7
Deferred Maintenance	8
Audit Trails.....	9
Version Control	10
Program Documentation	10
CONCLUSIONS	11
RECOMMENDATIONS.....	11
CHAPTER II: SECURITY.....	13
ACCESS TO PROGRAMS AND DATABASES	13
RIMS ACCESS.....	15
SECURITY POLICIES	15
CHAPTER III: APPLICATION CONTROLS	17
SOURCE DOCUMENTATION.....	17
PROCESSING CONTROLS	18
ERROR DETECTION AND CORRECTION.....	20
CHAPTER IV: OTHER MATTERS FOR CONSIDERATION.....	23
COMPUTATION OF MONEY MATCH LUMP SUM BENEFITS	23
PRINTER PURCHASE.....	24
ACCOUNTS RECEIVABLE MANAGEMENT.....	24
COMMENDATION.....	26

	<u>Page</u>
AGENCY’S RESPONSE TO THE AUDIT REPORT	27
AUDITS DIVISION’S COMMENTS ON THE AGENCY’S RESPONSE TO THE AUDIT REPORT	41
APPENDIX A: COBIT™ OBJECTIVES RELATING TO SDLC METHODOLOGY	47

SUMMARY

BACKGROUND

The Oregon Public Employees Retirement system (PERS) is responsible for managing a retirement system for state and local governments in Oregon. As of June 1999, PERS served approximately 194,000 active members and 78,000 retirees. Generally, PERS relies on its computer-based Retirement Information Management System (RIMS) to perform many of its retirement service functions.

RIMS consists of several sub-systems including the Benefit Calculation Sub-System (BCSS), which calculates member retirement benefits and the related adjustments to various reserve accounts. PERS developed and implemented RIMS between 1986 and 1991 at a cost of approximately \$8.25 million. Currently, PERS is involved in a system development project to replace RIMS.

The RIMS operates on the Department of Administrative Services mainframe computer. Employees of the PERS Information Services Division maintain and operate the system.

SCOPE AND PURPOSE

The purpose of this audit was to evaluate the controls governing the RIMS Benefit Calculation Sub-System (BCSS) and any associated work-arounds. Major objectives included evaluating the agency's policies and procedures governing system development, security, and application controls. Application controls are those used to ensure that data remains complete, accurate, and valid during input, processing, and output. We reviewed policies and procedures in use between July 1999 and March 2000.

AUDIT RESULTS

PERS's policies and procedures are not sufficient to control new system development or the day-to-day maintenance of its computer-based systems. Thus, the business risks associated with its current system development project appear significant. Those risks include an increased likelihood that the new system will not meet user requirements, provide adequate control or allow for effective future modifications. Additionally, the risk is greater that PERS will not be able to adequately maintain RIMS during the development process or the new system, once implemented.

Security measures also do not sufficiently restrict access to systems and databases.

Additionally, BCSS application controls do not ensure that transactions processed through the system remain valid during data input, processing, and output. Improvements should include control, tracking, and storage of source documents; controls to prevent and detect errors during processing; and controls over error correction.

During our audit we also noted other matters of concern including an anomaly in PERS's methodology for computing one type of retirement benefit, an inappropriate printer purchase, and issues relating to accounts receivable management.

RECOMMENDATIONS

- Develop and implement a comprehensive System Development Life Cycle (SDLC) methodology before proceeding further with new system development plans.
- Improve security over system programs and data files and user access to the system. This should include developing, updating and training users on security policies and procedures.
- Control and track source documents and ensure that they are properly retained in compliance with records retention schedules.
- Implement controls, either automated or manual, to mitigate risks associated with existing RIMS deficiencies. In particular, ensure that out-of-balance transactions are timely identified, investigated, and appropriately resolved.
- Correct the method of calculating lump sum money match retirement benefits, enforce purchasing policies, and ensure that accounts receivable are managed in accordance with state laws and regulations.

AGENCY RESPONSE

The Oregon Public Employees Retirement System's response to this audit report begins on page 27 of this report. The Audits Division's comments regarding that response begins on page 41.

INTRODUCTION

The Oregon Public Employees Retirement System (PERS) is responsible for maintaining a retirement system for state and local governments in Oregon. PERS administers a defined benefit retirement plan that specifies the amount of benefits it will provide to its members according to various factors such as age, years of service, and compensation. There are a number of retirement options for members. The agency provides service and disability retirement income, and death benefits to its members and their beneficiaries. A board of eleven trustees oversees PERS operations. The board appoints the PERS executive director, who manages the day-to-day operation of the agency.

To be a member of PERS, individuals must have been, or currently are, employed by a participating agency or government and must have contributed to the system. Both members and employers contribute to PERS. Member contributions are set by statute and are individually accounted for in a reserve account that earns interest. The amount of interest earnings posted to an individual member's balance depends on the program or option that he or she has elected to take. Employer contributions are also accounted for in a reserve account. The employer reserve does not separately track amounts contributed on behalf of individual members; rather, it accounts for the total amounts paid into the reserve by each employer. Employer contribution rates are based on actuarial formulas that estimate amounts that will be required to assure that the system has adequate funding.

When a member retires, the related member reserve balance is moved into a benefit reserve account to fund that portion of the benefit. In addition, a sufficient amount to fund the remainder of the retirement benefit is transferred from the employer reserves into the benefit reserve account. The benefits reserve account is recorded in aggregate and is used to fund future benefit payments.

As of June 1999, there were more than 194,000 active members and more than 78,000 retirees in PERS. For fiscal year 1999, PERS collected more than \$338 million in contributions from members and approximately \$510 million in contributions from employers. During that year, PERS paid more than \$1.4 billion in benefits and refunds to its members. Net assets held in trust for pension and postemployment benefits totaled more than \$35 billion.

Generally, PERS relies on the Retirement Information Management System (RIMS) to perform many of its retirement service functions. This computer-based system is comprised of several sub-systems that track member status, calculate benefits, and record employer contributions. One important component of RIMS is the Benefit Calculation Sub-System (BCSS), which was implemented in October 1988. The BCSS calculates member retirement amounts and passes this information to the Benefit and Pension Sub-System. The BCSS also calculates adjustments to various reserve accounts.

The RIMS operates on the Department of Administrative Services mainframe computer. PERS implemented RIMS between 1986 and 1991 at a total cost of approximately \$8.25 million. Employees of the PERS Information Services Division (ISD) maintain and run the system.

INFORMATION SYSTEMS CONTROLS

Information system controls are generally categorized as general or application controls. General controls are those controls that protect the environment in which all application software operates. Application controls are designed to reduce the risk of unauthorized, inaccurate, or incomplete input, processing, output, and storage of transactions for a specific application.

SCOPE AND METHODOLOGY

This audit is an application controls review of the RIMS Benefit Calculation Sub-System (BCSS) and its associated work-arounds. The audit had the following major objectives:

- Determine if controls are in place to ensure that program changes to RIMS systems are managed to minimize the likelihood of disruption, unauthorized alterations, and errors. Additionally, determine if the procedures governing system development and maintenance are adequate to ensure that the systems meet user needs.
- Determine if the controls over the BCSS appropriately restrict access and adequately protect the system and data from unauthorized creation, use, damage, or loss.
- Determine that the controls over the BCSS, and related manual processes, provide reasonable assurance that:
 - The data entered is complete, accurate, and valid;
 - All data is processed completely and accurately; and
 - System output is protected and distributed properly.

We performed our fieldwork between July 1999 and March 2000. To achieve our audit objectives we interviewed agency staff. Additionally, we reviewed procedures, system documentation, internal audit reports, and other relevant documentation to identify and evaluate risks and controls. We also designed and performed procedures to determine if the selected controls existed or were working as intended.

During our audit we used the Information Systems Audit and Control Foundation's Control Objectives for Information and

Related Technology (COBIT™) to identify generally accepted and applicable control objectives and practices for information systems. ISACF is a worldwide organization dedicated to researching and promulgating generally accepted information systems control objectives and audit guidelines.

We conducted our audit in accordance with generally accepted government auditing standards.

CHAPTER I: SYSTEM DEVELOPMENT AND MAINTENANCE

The Oregon Public Employees Retirement System (PERS), in conjunction with contractors, implemented the Retirement Information Management System (RIMS) between 1986 and 1991. Since then, employees of the PERS Information Systems Division (ISD) have been responsible for its maintenance. One of the challenges that accompanies these responsibilities is legislatively mandated changes to PERS retirement plans. This environment of change emphasizes the need for PERS to have sound policies and procedures to govern how it will develop and maintain its systems. 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 those policies and techniques to ensure that all phases of system development and maintenance are adequately addressed.

Currently, PERS is involved in a project to replace RIMS. In part, this work is necessary because RIMS currently lacks the functionality that PERS needs to adequately fulfill its business requirements. When processing new retirements, PERS employees must use alternate procedures to work around processes that RIMS cannot successfully complete. PERS also continues to rely on data stored in the system that RIMS replaced approximately nine years ago because the data was not all converted and integrated into RIMS databases. Additionally, RIMS lacks sufficient edits to ensure that data will be completely and accurately entered and processed by the system. The current condition of RIMS is symptomatic of applications developed and maintained without an adequate SDLC methodology.

SDLC METHODOLOGY

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 a structured SDLC methodology reduces the likelihood that disruptions, unauthorized alterations, or errors could be introduced into the system.

PERS management is ultimately responsible for the acquisition and maintenance of software that it needs to satisfy its business requirements. To do this, PERS should define and implement information system standards and adopt a system development life cycle methodology to govern acquisition, implementation and maintenance processes.

For SDLC methodologies to be effective, they should be written, require specific deliverables for the various project phases, be understood by all parties, and be approved and enforced by management. Before October 1999, ISD's limited procedures relating to SDLC were generally unwritten. Its methodology then consisted of a quality assurance plan that broadly discusses quality assurance goals and objectives, and a few separate written procedures. These methodologies do not adequately address most of the necessary SDLC elements. Some of the key aspects not covered in PERS's SDLC methodology include the following:

- Standards covering testing requirements, verification, documentation and retention.
- Procedures to formally and effectively categorize and prioritize proposed system modifications.
- Procedures to assure that adequate audit trails exist.
- Mechanisms and procedures to provide adequate version control.
- Procedures to ensure that all aspects of the SDLC are adequately approved and documented.
- Mechanisms to provide for adequate application controls that ensure the accuracy, completeness, timeliness, and authorization of inputs, processing, and outputs.

Many potential risks arise when adequate SDLC methodologies are not used when developing a computer-based system. The first and most devastating risk is that the completed system may not meet the users' business needs, user requirements, and expectations. Although following an adequate SDLC methodology reduces many of the risks associated with system development and maintenance, it does not absolutely ensure that projects will be successfully completed. Other factors such as funding restrictions, technical expertise of staff, and management or user involvement also play a major role in the success of system development and maintenance.

EFFECTS OF INCOMPLETE SDLC

Testing Standards and Requirements

One important aspect of SDLC methodologies is that they should provide standards for software testing. In addition, these methodologies should ensure that programmers performing tests are adequately supervised, their work monitored, and their access rights sufficiently limited to avoid inadvertent or unauthorized modification of programs or data. Thus, programmers' work should be performed in a controlled environment separate from the normal operating regions of the system.

PERS SDLC standards and procedures do not adequately address these important issues. For example, during 1998 an ISD programmer performed a test to ensure that programming changes properly resolved errors that existed in the RIMS system code. An employee from the System Development Team verified that the testing plan would achieve the desired results and provided the programmer with member accounts to use for the test. However, the programmer did not perform the test according to the plan. Rather, she inadvertently created a file containing data normally used by RIMS for printing and disbursing retirement benefit checks. Since the test was conducted in an area not adequately segregated from live production files, it was processed according to normal procedures. During a two-day period, several invalid check files were sent to the Department of Administrative Services print shop for printing and distribution.

Consequently, 19 checks totaling approximately \$602,000 were inadvertently printed and distributed to members. Of those checks, nine totaling approximately \$273,000 were cashed by the recipients. Although the moneys from the checks that were cashed were returned to PERS, the agency lost approximately \$4,100 in interest that would have been earned if the incident had not occurred. Of the 10 checks that were not cashed, nine were returned to PERS. The remaining check for approximately \$19,000 has neither been cashed nor returned.

The problem was not immediately detected by PERS employees. A member recognized that the checks PERS mailed to her were unusual and she called PERS to inquire about the discrepancy. Similar problems have occurred in the past during

tests of program changes. During those tests, however, PERS employees intercepted the checks before they could be mailed.

These incidents occurred because ISD managers did not provide adequate supervision to ensure that the testing plans were correctly performed or that the programmer fully understood her responsibilities. Additionally, the agency's SDLC did not specifically provide methodologies to ensure that programmers only operated within a controlled testing environment. Furthermore, PERS SDLC does not require that testing results be adequately documented and retained. Consequently, PERS managers could not readily verify whether all the checks involved in the error were accounted for, and either returned to PERS or the moneys reimbursed. Therefore, PERS sent letters to individuals believed to possibly have received the checks asking them to return any extra checks they had received.

Following these incidents, PERS implemented measures to lessen the risk that benefit checks could be inadvertently mailed to members during such tests; however, the underlying cause has not been addressed. PERS SDLC methodologies do not ensure that programmers can perform tests only within a controlled test environment; tests are appropriately approved, designed and documented; and programmers are adequately supervised. Therefore, the risk still exists that uncontrolled tests may produce unintended results and go undetected.

Deferred Maintenance

An important objective of SDLC methodologies is to provide a comprehensive framework of policies and procedures for developing, implementing, and maintaining systems. When adequate SDLC methodologies are in place, systems are less likely to fall into disrepair or experience early obsolescence.

PERS brought RIMS modules online between 1986 and 1991. By 1996, the agency had approximately 650 outstanding requests to modify or enhance the system or correct errors in the code. Some of these outstanding issues dated back to 1989 and included requests to fix code relating to core business functions, such as calculating benefits for various retirement options. Because the system cannot accurately perform these calculations, PERS employees have to perform those processes using manual work-around procedures. By 1997, agency managers indicated that the RIMS system should be replaced because the cost of repair would exceed the benefit. Thus, they deferred work on approximately 490 existing requests for RIMS

system changes and indicated that the new system being developed to replace RIMS would resolve those issues.

Manual work-arounds interrupt normal processing cycles and increase the risk that errors could occur. Normal processing cycles are delayed when PERS routinely stops processing to accommodate manual work-arounds. During 1998, manual work-arounds contributed to known errors that resulted in approximately \$412,000 of duplicate payments to retirees (this is described further in Chapter III). Furthermore, manual work-arounds contribute to backlogs of unreconciled transactions in various accounts. For example, as of October 1999 one account used to record certain member reserve transactions included approximately \$33 million in unreconciled transactions (further details are in Chapter III). During 1998 the agency requested authority from the emergency board to spend an additional \$94,000 to resolve some of the errors contained in these databases. The request was granted, and the project to correct the databases began in 1998. Due to the high volume of retirements that PERS was processing during that time, the workers hired to investigate and resolve the database problems were diverted from the project and reassigned to process retirement backlogs.

Audit Trails

In developing systems, management should ensure that programs include audit trails. To be sufficient for users' needs, audit trails should indicate by whom and when transactions were initiated, approved and completed, as well as the transaction's detail. This allows data reconstruction if the program is disrupted.

PERS employees indicate that RIMS does not have adequate audit trails for employees to effectively track transactions. One PERS manager indicated that microfilmed documents are the only means for tracing some transaction histories. During our review, we found it difficult to follow transaction histories and track changes to employer reserves and member accounts. Some transaction entries directly change account balances, thus leaving no electronic history or audit trail of the adjustment.

This situation exists because RIMS developers did not adequately consider audit trail requirements during the design of the system. Subsequent work requests to correct these deficiencies have been set aside until PERS replaces the system. In the meantime, many routine RIMS inquiries still require

employees to manually trace transactions through microfilmed documents. Current PERS SDLC policies and procedures do not ensure that future system development projects or modifications will adequately consider audit trail needs or requirements.

Version Control

Another important aspect of SDLC methodology is ensuring that only authorized changes are made to programs. To accomplish this, management should have procedures and mechanisms to control and track changes that are made to the software. Furthermore, programmers' access rights should be appropriately limited.

ISD's process for controlling and tracking software updates does not provide version control. For example, ISD does not monitor the various RIMS program modules to ensure that only the most current authorized versions are in production and that subsequent versions do not unintentionally negate previous programming changes. One PERS manager indicated that the latter circumstance occasionally occurs.

These issues exist because PERS SDLC methodologies do not include specific written procedures for maintaining version control or specify who is responsible for tracking program changes.

Program Documentation

SDLC methodologies should include provisions for creating and updating system documentation and requirements, program specifications, operations manuals, etc. In addition, organizations should create and retain documentation of significant SDLC processes and approvals as they occur, such as software testing plans and results of those tests. Documentation should be sufficient to guide and direct employees as they use or modify the system.

Because PERS does not require employees to create or retain sufficient documentation of system development and maintenance activities, RIMS documentation is incomplete, fragmented, and generally out-of-date. Additionally, ISD has not maintained an operations manual for the system. As a result, PERS has an increased risk that operators and programmers may introduce errors into the data or programs

because they do not fully understand key system requirements or attributes.

CONCLUSIONS

In the past, PERS lacked adequate SDLC methodologies to effectively govern its development and maintenance processes. As a result, the RIMS system did not satisfy the organization's business requirements. This is evidenced by the various manual work-arounds that became necessary to process routine retirement transactions. More importantly, the \$8.25 million application evolved from a newly developed system in 1991 to a state of near obsolescence by 1996 with approximately 650 outstanding requests for system modifications. PERS management later decided to set aside the change requests and address the problems with a new system.

PERS management recently developed an SDLC methodology; however, it is written at a high level that is not sufficient to govern system development or day-to-day maintenance. The effects of insufficient SDLC methodologies are apparent. RIMS does not support PERS's core business functions and has not for a number of years. Based on PERS's current SDLC methodology, we conclude that the business risks associated with the agency's system development project are significant. Some of those risks include an increased likelihood that the proposed system will not include all the necessary elements to meet user requirements, provide adequate control or allow for effective future development and maintenance modifications. Additionally, the risk is greater that PERS will not be able to adequately maintain RIMS during the development process or the new system, once implemented.

RECOMMENDATIONS

We recommend that PERS develop and implement a comprehensive SDLC methodology before proceeding further with system development plans. This methodology should include specific policies and procedures to govern all aspects and phases of the system development life cycle, including the following important elements:

- System design requirements and methodologies.
- Standards covering testing requirements, verification, documentation and retention.

- Procedures to formally and effectively categorize and prioritize proposed system modifications.
- Procedures to assure that adequate audit trails exist.
- Mechanisms and procedures to provide adequate version control.
- Procedures to ensure that all aspects of the SDLC are adequately approved and documented.
- Mechanisms to provide for adequate application controls that ensure the accuracy, completeness, timeliness, and authorization of inputs, processing, and outputs.

The resulting SDLC methodology should conform to generally applicable and recognized industry standards, such as those found in COBIT™. A list of COBIT™ control objectives addressing SDLC methodologies is included in Appendix A.

CHAPTER II: SECURITY

Management has a responsibility to ensure that its assets are protected against unauthorized use. For electronic data, this is accomplished by limiting access to read and change the files through what are known as logical access controls.

Generally, management specifically assigns responsibility for overseeing security access. This would include responsibility for establishing individuals access as authorized by management, monitoring security access violations, initiating reviews to ensure that the granted access remains valid, removing invalid users, and otherwise exercising control over this function.

PERS management has not adequately emphasized security for RIMS. PERS does not have a comprehensive set of policies and procedures, and has not assigned to the Security Officer the responsibility for security which includes monitoring access violations and periodic review of access privileges to ensure they remain appropriate.

ACCESS TO PROGRAMS AND DATABASES

Restricted access to a system's programs and databases is essential to ensure the integrity of the system. Access to these files should be based on an individual's demonstrated need to view, add, change, or delete programs or data. Without this control, there is the increased risk of unnecessary or unauthorized access which intentionally or unintentionally modifies programs or data. This can then result in unauthorized or unintended processing of data.

Our review revealed a lack of monitoring access privileges that had been granted to the RIMS databases and program libraries. The Information Services Manager stated that there were no formal procedures for granting access to the databases or program libraries, monitoring of access, and documenting who was granted access or why. Without monitoring of access granted there is an increased risk that individuals may have greater access than is required to perform their jobs, or that individuals who no longer work for the agency may continue to have access.

The test region is a segregated area set aside for programmers to make and test program changes before moving them into production. We identified the following issues related to test and production access at PERS.

- Of six users with the ability to alter production program code, three were not based on a demonstrated need, such as to move revised program code from test into production.
- Of 80 users with authority to alter at least one production dataset, most had greater access authority than needed to perform their duties.
- Of the 64 users with the ability to alter programs in the PERS test region, 35 should not have this access because they do not work in units responsible for system development and maintenance.
- For one sensitive production dataset, PERS indicated that no one had access to modify this file. Our review of access rights found that 19 users actually had authority to alter this dataset. Of these, 13 were from the Department of Administrative Services (DAS), and were not PERS employees.

Within the above totals, there are 88 unique users with the ability to alter at least one PERS program or dataset. The demographics of these IDs are as follows:

- 54 were PERS employees or contractors.
- 31 were from DAS.
- Three were not specifically assigned to an individual and thus do not allow assigning responsibility for actions taken using the IDs.

These conditions exist because PERS has not maintained and enforced effective policies and procedures for maintaining security over RIMS program files and data.

We recommend that PERS develop policies and procedures to establish and maintain effective security over its programs and data files. Users should be granted the minimum amount of access to perform their job functions. PERS should maintain and periodically review reports detailing the users that have access to the data files and programs. Currently existing unidentified or unauthorized personnel's access should be immediately revoked. Current generic IDs should be eliminated. PERS should reach a formal agreement with DAS that limits the number of DAS employees with the ability to access and alter PERS data and programs.

RIMS ACCESS

PERS management does not always properly grant or effectively monitor user access to RIMS. In addition, management does not review security reports for unauthorized access attempts or other potential security violations.

As of December 1999, there were 311 RIMS user IDs. Of those, 120 were inappropriate because they were not specifically assigned to an individual, were former employees, or were unknown users.

These conditions exist because PERS has not ensured that those assigned responsibility for logical access security for RIMS properly grant and maintain security.

We recommend that PERS specifically assign responsibility for ensuring that logical access security for RIMS is properly granted and maintained, and security reports reviewed. Management also should ensure that user access privileges are regularly evaluated for appropriateness. Unidentified or inappropriate access should be immediately revoked.

SECURITY POLICIES

Security policies and procedures are intended to safeguard information against unauthorized use, disclosure, modification, damage, or loss. Management should implement logical access controls to ensure that access to systems, data, and programs is restricted to authorized users. These controls should be applied to everyone authorized to use the computer system, whether they are employees of the organization or not.

For security controls to be successful, their purpose must be clearly defined and communicated to system users. A written security policy is an essential component in heightening the security awareness throughout the organization. This security policy should demonstrate management's commitment to security, including an access philosophy of "need to know" as the basis for access, proper access authorization procedures, and periodic reviews of access privileges. This policy should be coupled with implementing procedures to inform and educate users on their roles and responsibilities.

PERS management has not established an adequate framework of policies and procedures to safeguard information against unauthorized use, disclosure, modification, damage, or loss.

Examples of items missing from this framework include procedures governing reviews of access violations and responsibility for ensuring that such procedures are developed and maintained.

We recommend that PERS management specifically assign responsibility for developing and updating security policies and procedures. A security manual for users should be developed and distributed to convey the policies and procedures to all PERS employees.

CHAPTER III: APPLICATION CONTROLS

Application controls reduce the risk of unauthorized, inaccurate, or incomplete input, processing, output, and storage of transactions. These controls include methods of ensuring that only complete, accurate, and valid data are entered in a computer system; processing performs the correct functions and results are accurate; and data are properly maintained. The controls can be either manual or automated processes.

Inadequate application controls can result in incorrect processing including computational errors; partial, duplicate, or incomplete processing; unauthorized processing; and lost or compromised data.

We found that the system of controls established by PERS management for the Benefit Calculation Subsystem (BCSS) does not appear sufficient to mitigate those risks. Areas where application controls should be improved include controls over data inputs, controls to prevent or detect processing errors, and controls to ensure effective and timely error detection and correction.

SOURCE DOCUMENTATION

Management is responsible to establish, maintain, and enforce policies and procedures to ensure that all authorized source documents are complete and accurate, properly accounted for, and transmitted timely for data entry. They are also responsible for establishing procedures to ensure original source documents are retained, or are reproducible, for an adequate length of time to facilitate retrieval or reconstruction of data as well as to satisfy legal requirements. PERS's record retention schedules require that member transaction data be retained for 175 years.

Our review indicates that PERS policies and procedures do not require that staff establish control over retirement packets upon receipt, maintain control through processing, and ensure all source documents reach permanent storage. The agency does not use logs, transmittal documents, or other means to ensure the correct and timely handling of all source documents.

PERS cannot provide reasonable assurance that all member information is completely recorded to support completed transactions. We found the following instances in which standard documents for a member's transactions were not retained in the permanent microfilmed record:

- A data modification worksheet detailing the changes made to the benefits reserve for one retirement was missing from the microfilmed records.

- Worksheets detailing the manual calculations for another retirement were not microfilmed.
- Several significant documents relating to the closing of a member's account were missing.
- The original notice of entitlement was not microfilmed for another retirement.

Because of the poor audit trail in the RIMS (see Chapter I), PERS employees rely on the microfilmed documents to understand and trace transactions in the system. Therefore, it is critical that PERS microfilm and properly reference all relevant documents.

We recommend that PERS implement policies and procedures to ensure that each retirement packet is logged upon receipt and tracked throughout processing and microfilming, including reconciliations of packets received to packets processed and packets microfilmed. Further, steps should be taken to ensure that all documents are microfilmed and retained in accordance with the record retention schedules.

PROCESSING CONTROLS

Management is responsible for designing and implementing controls to prevent, or detect and correct processing errors promptly. The standard applies to either automated or manual processes, and includes the following elements:

- Adequate segregation of duties,
- Routine verification of work performed,
- Batch controls and balancing,
- Data validation and edit controls, such as limit, range, duplicate, and reasonableness checks,
- Master file update controls,
- Error identification and handling routines, and
- Audit trails to facilitate tracing transaction processing and reconciliation of disrupted data.

We found that BCSS does not provide reasonable assurance that benefits will be processed accurately and in a timely manner for the following reasons:

- PERS employees must interrupt BCSS job processing streams to modify data or remove transactions from the processing cycle for manual benefit calculation.
- BCSS does not automatically identify and/or exclude some transactions for which manual intervention is required.
- PERS has not sufficiently documented its procedures to ensure that all required manual processing actually occurs.
- PERS has not documented the error codes, and underlying edits contained in the BCSS. Thus, it does not have the related documentation of actions needed to resolve these errors.
- PERS does not retain error reports generated by BCSS to document the problems that occurred and action taken to correct the problems.
- PERS does not use batch controls. The control totals generated by BCSS are not used to ensure that benefits are processed accurately and completely.
- PERS has not established controls, either automated or manual, to prevent or detect retirement applications processed more than once other than when it happens in the same automated batch.
- Although independent verification of manual processing is required, it is not always performed and at other times is not effective to ensure an accurate benefit calculation.
- The staff responsible for “verifying” input to the automated system does not review source documentation.
- PERS does not have effective policies and procedures requiring that processing controls be documented and evaluated during system development or maintenance.

Consequently, duplicate payments have occurred and went undetected for approximately two years. Five of the duplicate payments detected by PERS totaled more than \$412,000 and cost the fund at least \$170,000 in lost interest earnings. We

calculated the amount of lost interest based on the Tier 1 amounts available for distribution, which are established by PERS. Through our analytical procedures, we identified two more duplicate payments totaling about \$86,000 that had remained undetected since 1997.

We recommend that PERS assess the risks associated with the existing RIMS processing deficiencies, such as those described above, and implement controls, either automated or manual, to mitigate those risks.

ERROR DETECTION AND CORRECTION

PERS management is responsible for ensuring that procedures are in place to detect and correct errors in a timely manner.

Using RIMS reports, PERS generates a detail listing of out-of-balance transactions. However, management does not ensure that each item is investigated and properly corrected on a timely basis. There was no regular review and follow up of unreconciled items, which a December 1997 PERS internal audit report identified as totaling more than \$31.7 million.

The legislature's Emergency Board provided approximately \$94,000 of increased limitation for two temporary staff to perform data cleanup, including these out-of-balance transactions. The project ended in October 1999; however, out-of-balance transactions totaled more than \$33 million at the close of the project. Some of the individual out-of-balance transactions have been unresolved since 1991.

Further, PERS management has not ensured that proper corrections are made to reserves when out-of-balance transactions are being resolved.

For the adjustments we reviewed, PERS adjusted the member reserves but did not correct charges to employer's reserves. Thus, the charges to employer reserves were overstated by over \$420,000. Charges to the employer's reserves increase the unfunded liability, and thus may increase the rate PERS charges the employer.

We recommend that PERS ensure that all out-of-balance transactions are identified, investigated, and resolved in a timely manner. These procedures should ensure that member, employer, and benefit reserves are corrected. Written

procedures should assign responsibility for correcting errors, including documentation standards and supervisory reviews.

CHAPTER IV: OTHER MATTERS FOR CONSIDERATION

While performing our application control review we noted other conditions which, while not directly related to our audit objectives, are matters of concern.

COMPUTATION OF MONEY MATCH LUMP SUM BENEFITS

When a member retires and selects a lump-sum settlement, the member receives the member's account balance in one or more installments. The member also will receive an annuity for the employer's share of the retirement benefit. The lump-sum payment will include interest through the date it is distributed. Generally, the annuity is computed as of the date of retirement. The annuity payments are made retroactive to the date of retirement, so that if payment is delayed the retiree will still receive annuity payments for those months.

During our review, we noted that for retirements calculated using the lump sum money match (LSMM) method, PERS charges the employer's reserve and calculates the annuity using the date of distribution rather than the date of retirement. This, in effect, pays the retiree interest for the delay period and includes the interest in the annuity calculation. PERS management acknowledges that this is the only type of retirement method in which it uses the date of distribution for an annuity calculation. As the date of distribution can be considerably after the date of retirement (six months in one of the computations we tested), the effect on the charge to the employer can be significant.

PERS indicated that 2,131 members selected the LSMM retirement option during 1998 and 1999. We recalculated six of those retirements, which are not necessarily representative, using the retirement date rather than the date of distribution. For those six accounts the employers were charged approximately \$44,000 more by using the date of distribution for the calculation rather than the date of retirement.

We recommend that PERS change its method of calculating LSMM annuity calculations to make it congruent with the other annuity calculations. Retirement benefits that PERS calculated under the previous method should be recalculated and the associated employer reserves corrected. PERS should also

consult with the Attorney General's office regarding the possible recovery of benefit overpayments from the retirees.

PRINTER PURCHASE

PERS procurement policies and procedures require employees to consider state price agreements before making purchases. If a direct purchase is made from a non-price agreement vendor, evidence of that consideration must be documented. The policy also strictly prohibits making direct purchases without prior authorization of the Auxiliary Services Manager. These policies and procedures help to ensure that price competition occurs and that vendor selection is made objectively.

During October 1999, the Information Systems Administrator purchased a used printer for the agency for \$3,000. The administrator purchased the printer directly without the approval of the Auxiliary Services Manager. Additionally, he purchased the item from another PERS employee; this same person is listed as his PERS retirement beneficiary.

The need for the printer is unclear because a similar printer is located in close proximity to the one purchased, and the only employee using the printer is the employee who sold it to PERS. The printer was manufactured in 1996, and the model is no longer sold as new in the United States. A new printer of equal or higher quality sold for approximately \$2,000 at the time the manager purchased the used printer.

Although the PERS Fiscal Operations Manager subsequently approved the purchase, it violated PERS purchasing policy and was not made in the best interest of the state; PERS managers therefore spent at least \$1,000 more for the printer than was necessary.

We recommend that PERS management enforce its purchasing policies.

ACCOUNTS RECEIVABLE MANAGEMENT

Oregon Revised States 293.229 to 293.245 requires all state agencies to make reasonable efforts to collect the full amount of moneys owing. These efforts include assigning delinquent accounts to the Department of Revenue or, according to the 1999 law, to a private collection agency for recovery. PERS

management is ultimately responsible for establishing adequate policies and procedures to ensure that receivables are collected in full, and in a timely manner. Those receivables deemed uncollectible should be written off in accordance with state laws.

During our review, we found that PERS accounts receivable have not been properly managed or supervised. PERS does not send monthly statements beyond the 90-day past due notice, nor is any other action taken on these overdue items. No receivables have been written off or referred to a collection agency in several years. More than 65 percent of the receivables, \$748,000 of the \$1.14 million balance at November 30, 1999, are over 90 days past due. Accounts totaling \$541,000 had not received any payments in over a year.

PERS management indicated that the amount of the receivables was not considered significant and, therefore, they had not been closely monitoring the collection of these receivables.

We recommend that PERS implement procedures to ensure that accounts receivable are managed in accordance with state laws and regulations.

COMMENDATION

The courtesies and cooperation extended by officials and employees of the Oregon Public Employees Retirement System during the course of our audit were very commendable and sincerely appreciated.

AUDIT TEAM

Neal E. Weatherspoon, CPA, CISA, Audit Administrator

Mark A. Winter, CPA, CISA

Stanley Y. Mar

Nancy J. Winston, CPA, CISA

Ryan Dempster

Daniel Smith

Benjamin Wilson

AGENCY'S RESPONSE TO THE AUDIT REPORT



Oregon

John A. Kitzhaber, M.D., Governor

Public Employees Retirement System

Headquarters:
11410 S.W. 68th Parkway
Tigard, OR

Mailing Address:
P.O. Box 23700
Tigard, OR 97281-3700
(503) 598-7377
TTY (503) 603-7766

June 9, 2000

John N. Lattimer
State Auditor
Oregon Audits Division
255 Capital St NE Ste 500
Salem, OR 97310

Dear Mr. Lattimer,

I am enclosing our response to the Audits Division draft report regarding the Information Technology Application Control Review conducted at PERS from July 1999 to today. We appreciate the chance to offer our comments on specific portions of the draft report. In addition, by way of general comments I would add the following:

Cost and Benefits: Although the audit provided some findings and recommendations that PERS has found useful and is already responding to, we regret the expense of the audit in light of the benefits provided. The audit – originally estimated by the audit team at approximately \$80,000 – is now estimated to cost the PERS System close to \$300,000 in direct charges, before recognizing our internal costs of assisting the audit team. The direct expense to members proved to be 275% higher than expected. More than a year ago, we hired a third party consultant, Genesis Corporation, to do a gap analysis of PERS information technology skill sets, roles, methods, tools and approaches – including our software development policies (SDLC). This valuable \$28,000 investment produced multiple recommendations which are now firmly integrated into the development plans for the design and implementation of our new system, the successor to the aging legacy system, RIMS – the subject of the audit team's work.

Precision in Scope: The audit team did extensive fieldwork on the legacy system and its related policies. Given that the team announced at the inception of their effort that their focus was on RIMS, announced periodically during their many visits that their focus was on RIMS, announced in their pre-report briefing to the PERS Audit and Budget Committee that their focus was RIMS and once again noted in their draft report this same focus, we were not surprised to see findings and recommendations associated with their fieldwork on the legacy system and its associated policies. What was surprising was the team's decision to comment broadly on the new system – OPAS, which is in the early stages of planning and design, an area where we could not find evidence of any appreciable fieldwork.

Context, Balance and Perspective: In our meetings with the audit team we recounted the numerous instances in which we were largely in agreement with their facts and recommendations. However, as detailed in the enclosed response, there were important aspects of the issues discussed by the audit team that the draft report failed to note. These aspects will help all readers – laypersons as well as experienced IT professionals – better understand both the concerns raised as well as the corrective actions taken.

Thank you again for the opportunity to comment on the report and work with your team to improve the information technology effort at PERS.

Sincerely,

A handwritten signature in black ink, appearing to read "James Voytko". The signature is fluid and cursive, with a long horizontal stroke extending to the left.

James Voytko
Executive Director

Introduction

The Audits Division announced its intent to perform an information technology review of PERS's Retirement Information Management System (RIMS), specifically the Benefit Calculation Sub-System (BCSS). This review was scheduled to take 3-4 months beginning in July 1999 and cost approximately \$80,000. PERS staff provided all information requested in the context stated by the audit team. Audit fieldwork continued into May of 2000 and billed costs to date exceed \$250,000. Current estimate of total cost is approximately \$300,000. Until the April 2000 PERS Audit and Budget Subcommittee meeting, PERS was unaware that the team had any intention of extending its fieldwork into the OPAS development project. To our knowledge, no comprehensive fieldwork was performed nor audit evidence compiled sufficient to draw any supportable conclusion regarding the risks associated with PERS's new development project or its prospects for successfully meeting its objectives. Neither the project manager nor any key project staff were interviewed regarding the development procedures in place or under development within OPAS. When evidence supporting OPAS conclusions was requested by PERS staff, the audit team was unable to produce evidence that would support their statements related to our OPAS development efforts. Furthermore, the scope stated in this audit report confirms numerous verbal statements made by the audit team that the review performed is of RIMS BCSS, not of ongoing development efforts. Therefore, PERS feels that any comments related to OPAS development efforts unrelated to RIMS are unsupported, which could diminish the foundation of the audit conclusions of this report as a whole.

PERS acknowledges that RIMS was developed in the late 1980's and maintained since then in a less than optimal manner – we indicated that to the audit team before the review commenced; it is this knowledge that has led us to plan and refine our development activities (which have yet to progress beyond planning and initial design) with extraordinary care. We welcome a review that would validate our efforts in this area, but such a review has not been performed by the Audits Division.

The remainder of our comments address the audit findings in the RIMS context.

Chapter 1 – System Development and Maintenance

SDLC Methodology

The report notes that poor and incomplete Systems Development Life Cycle (SDLC) methodologies at PERS since RIMS was developed have created problems and recommends the development of a comprehensive SDLC.

Management Response:

PERS agrees. Inadequate SDLC methodologies have plagued software development in the RIMS environment. As we have shared with the audit team on numerous

occasions, we are dissatisfied with problems that have arisen over RIMS's lifecycle and agree that inadequate SDLC procedures are at least partly responsible for many of the noted deficiencies.

The audit report attributes inadequate SDLC for a variety of problems in the RIMS environment, including a backlog of requested systems changes, documentation deficiencies, and other weaknesses. What the report fails to emphasize is that ineffective SDLC is but one of many factors that created the problems in the RIMS system, including the numerous legislative policy changes in the PERS system in recent years, the nationwide scarcity of technically skilled personnel, financial constraints, the critical need to selectively engage PERS RIMS staff in the OPAS reengineering project and the increasing numbers of members approaching retirement age, among other things.

The audit report also fails to note that it was a deliberate management decision to house our SDLC development work in the OPAS design work rather than in the soon-to-be-replaced RIMS environment. The reasons for this decision were many. The OPAS project and technology proposed requires a qualitatively different SDLC. The presence of skilled outside experts available to PERS in the OPAS project but not in the RIMS environment presented by far the best opportunity for SDLC development work. The need for improved SDLC for RIMS is evident, but the payoff to housing SDLC work in the OPAS environment, targeted at the OPAS technology, promises benefits not just for the 3 to 4 years of life remaining in the RIMS lifespan, but multiples of that.

In addition, we believe the audit report is incorrect in stating that RIMS does not meet our business needs. We are well aware that RIMS does not do everything we would like, nor perform efficiently or effectively all of the time. Nevertheless, RIMS has been at the core of our operations for a decade; current workloads could not be processed within statutory timeframes without the assistance of RIMS. More than 60 percent of current retirements are processed through RIMS without any manual intervention required.

Corrective Action Proposed:

If PERS can devote resources to backward migrate the enhanced SDLC methodologies employed in the OPAS environment, *without introducing added risk into the OPAS project*, we will do so.

OPAS Project Risk

The audit report recommends that PERS develop and implement a comprehensive SDLC policy before proceeding further with new system development plans.

Management Response:

PERS disagrees. To accept the audit teams recommendation to stop work on all aspects of the OPAS reengineering project in order to complete just one important aspect of it would be so destructive that it must be ruled out. The agency and its contractors have spent 18 months assembling the legal, risk management, financial, and technical resources to launch the design phase of OPAS. Suspending work for any appreciable amount of time would introduce substantial and unnecessary risks, such as:

- Loss of key contractor technical personnel in a recruiting environment characterized by a painful scarcity of high level IT personnel
- Increase in project costs
- Delays in all ongoing and future phases of the project
- Quality control risks due to breaks in non-SDLC portions of the OPAS effort

Chapter 2 – Systems Security

Access to Programs and Databases

The report states that PERS has not maintained and enforced effective policies and procedures regarding security maintenance over RIMS program files and data.

Management Response:

PERS agrees. Many PERS security policies are outdated and are not effectively enforced. Also, management has neither aggressively monitored RACF access authority granted nor revoked unnecessary access in a timely manner.

In evaluating the necessity for PERS to maintain a minimum number of users with the ability to alter program code, the audit team failed to take into account operational and personnel requirements. Specifically, we indicated to the audit team that because RIMS operates on a 24-hour, 7- day-a-week cycle, it is necessary to have six users with the ability to alter program code. In order to provide coverage for holidays, vacations, and other absences as well as to rotate undesirable standby shifts, PERS has determined

that six users is the minimum number necessary to support processing requirements. The three users suggested by the report is simply unworkable and unreasonable.

The audit also mentions 80 users with the ability to alter programs or data, even though PERS has demonstrated that these users have no update authority, and therefore no ability to alter, to RIMS databases or programs. The users in question have access only to report files, not to program code or databases. PERS management does not consider these files to be production files; the audit team does consider them production files. Furthermore, comments related to DAS users should be directed to DAS. RIMS runs on the DAS mainframe, but PERS is not authorized to alter or revoke DAS user access.

Corrective Action Proposed:

PERS has reviewed the RACF security concerns raised by the audit team and taken corrective action where management deemed appropriate. PERS will investigate the 80 users with access to report files and take appropriate action where needed. In addition, PERS will evaluate its policies and procedures related to RACF security and evaluate the necessity of revisions in light of the audit recommendations. PERS will also request justification from DAS for all DAS users with access to RIMS production files.

RIMS Access

The audit report concludes that PERS has not ensured that those assigned responsibility for RIMS access appropriately maintain RIMS access security.

Management Response:

PERS agrees. PERS acknowledges that additional efforts need to be expended in monitoring RIMS user access.

Management agrees that review of access attempt security reports would be one effective means to determine if unauthorized persons have attempted to gain access to RIMS. However, PERS has determined that the RIMS lockout security feature, which disables a RIMS user account after five unsuccessful attempts is just as effective a security measure.

Corrective Action Proposed:

PERS will evaluate RIMS user access authority on a periodic basis and take any action necessary to ensure only authorized users have access to RIMS.

Security Policies

The audit concluded that PERS has not established an adequate framework of policies and procedures to safeguard RIMS information.

Management Response:

PERS agrees. PERS concurs that security policies and procedures currently in place are missing some key elements and have not been updated recently nor have they been distributed or emphasized sufficiently.

Corrective Action Proposed:

Policies and procedures are currently being reviewed and updated where necessary.

Chapter 3 – Application Controls

The audit report notes that the system of controls established by PERS management for BCSS does not appear sufficient to mitigate identified risks.

Management Response:

While PERS agrees that our application controls are not 100 percent effective, or even as effective as we would like them to be, the audit failed to provide a discussion regarding the degree to which this is a problem. PERS processes between 3,500 and 7,000 retirements a year, the vast majority of which have no problems associated with them whatsoever. Due to the extremely small sample size drawn by the audit team and the non-random nature of the sample, it is inappropriate to draw sweeping conclusions regarding the risks associated with the weaknesses noted. All controls involve a cost-benefit risk analysis. PERS has established effective processing controls and procedures considering financial, technical, and staff resources available.

Source Documentation

The audit report concludes that PERS cannot provide reasonable assurance that all member information is completely recorded to support completed transactions.

Management Response:

PERS disagrees. PERS acknowledges that we have less than optimal control over retirement packets and their associated workflows from “cradle to grave.” What the audit report fails to note is though the documents in question were not present in the microfilm files at the time of the audit team’s review, they were present in working files that were microfilmed at the conclusion of the work process. In the case of the “missing” documents noted, the records were in fact located in a working file in

another section. Finally, the last case noted by the audit report was microfilmed in 1990 and the record was available for review. Though the use of working files is not an optimal method of document control, there does not appear to be any basis for significant concern.

Corrective Actions Proposed:

PERS legacy system has provided us with invaluable experience and knowledge in document management and control processes. To accommodate ever-increasing document processing, archival, and retrieval demands and to better control the document process, new policies and procedures are being identified. PERS has also been looking at options to improve document controls by the use of new technologies. A new imaging prototype system will be tested in the near future, which will track documents and provide case management. This ancillary system has been identified as an important component in our new systems development efforts. A study has been performed on the applicability of this technology to RIMS. However, due to systems integration concerns, PERS has determined that it would be prohibitively expensive to implement such a system for RIMS and is now scheduled for inclusion in OPAS.

Processing Controls

The audit report states that BCSS does not provide reasonable assurance that benefits will be processed accurately and in a timely manner. It further notes seven duplicate payments were issued erroneously.

Management Response

PERS agrees that processing controls are not optimal and duplicate payments have occurred. However, the report does not place these problems in perspective. Although PERS recognizes the problems, the scope of these problems in relation to all payment functions conducted is highly immaterial. Duplicate payments are errors which are seldom made, which the audit team demonstrated with analytical procedures covering two years of lump sum payments. The instances noted were the only duplicates found and represent only .3 percent of the all lump sum payments issued in 1998 and 1999, and an infinitesimal percentage of the total number of payments issued by PERS annually.

Corrective Action Proposed:

PERS will evaluate the risks identified by the audit and implement cost-effective controls to appropriately mitigate those risks.

Five of the seven duplicate payments noted by the audit were detected by PERS and procedures were followed to initiate collection prior to the beginning of the audit. Collection procedures are in progress for the two additional overpayments detected during the course of the audit. In addition, PERS has prepared a change request to

prevent this type of problem in the future. In the meantime, since the duplicate payments belong to a similar benefit type, staff is taking extra steps in processing these types of payments to prevent recurrence.

Error Detection and Correction

The audit concludes that PERS has not ensured that out-of-balance transactions are identified, investigated, and resolved in a timely manner.

Management Response:

PERS agrees with the findings in regards to the few accounts that were selected and reviewed.

However, the report is incorrect in its assessment of the effectiveness of the data clean-up project and the implication of misuse of Emergency Board funding authority. PERS expended well over \$94,000 in staff and temporary resources, and the data clean-up project was highly effective in that it resulted in the clearing of over 1,800 items and posting over \$77 million in adjustments. We conducted a comprehensive review of the accounts reconciled by the data clean-up staff and found that the percentage of associated employer reserves that were out-of-balance was less than 1 percent.

An exceptional number of unreconciled accounts were added to the out-of-balance report because of a large number of corrections reported by employers during the 1998 and 1999 annual reconciliation process. This noteworthy increase in unreconciled accounts occurred during two years of exceptionally high numbers of retirements making the data clean-up project appear less effective than the actual results demonstrate.

Corrective Action Proposed:

On-line employer reserve transaction history has recently been made available to staff to aid in the out-of-balance reconciliation. As a result of staff research of selected accounts in this Audit Finding, a program problem was found that created errors under certain conditions. Final reconciliation of these accounts was completed in April 2000, and corrective action modifying this program was implemented on May 19, 2000. Upon passage of our budget in 1999, the Legislature had approved of a position to coordinate our ongoing efforts in the reconciliation of accounts and ensure timely accurate corrections.

Chapter 4 – Other Matters for Consideration

Computation of Money Match Lump Sum Benefits

The audit states that the calculation method used for Lump Sum Money Match benefits is inconsistent with other calculation methodologies employed by PERS. It recommends that PERS consider recalculating benefits calculated under this method, adjust employer reserves, recalculate benefits paid to retirees and make associated adjustments.

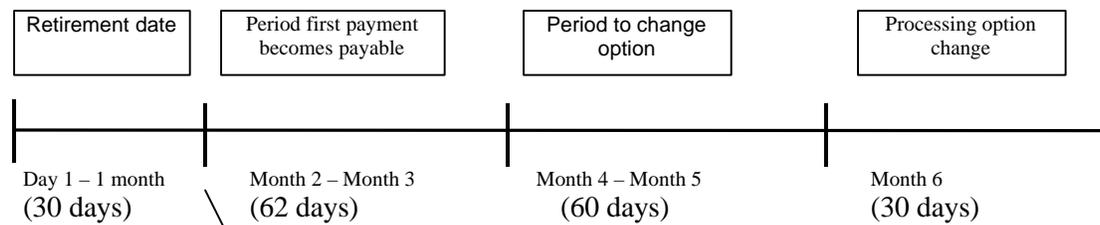
Management Response:

PERS agrees that the calculation methodology for the LSMM option is incongruent with other calculation methodologies. What the report fails to note is that the statute governing this option is extremely vague and subject to multiple interpretations. The audit also does not mention that PERS has discussed this issue with the Attorney General's office. PERS still maintains that the interpretation is a permissible interpretation of unclear statutory language. Therefore, no adjustments to reserves or retirement benefits are required.

The audit also did not provide a complete explanation of the causes for delay between retirement date and the date of distribution. As illustrated by the timeline below, the period between the effective retirement date and the final calculation of the lump sum benefit can, in some cases, span a six-month period. Under the Money Match method, the member's account (annuity plus earnings) is matched by an equivalent employer pension.

The one case noted in the audit report is not typical. The length of time to process this case was caused by a plan change. It's important to note most members do not elect to change their option. By statute, PERS is required to mail an estimated payment within 62 days of the payment due date. On average, 80 percent of service retirements are paid within 15 days of when the first benefit payment becomes due and 100 percent is paid within 62 days. According to statute, a member may elect to change their benefit option by written request that is made within 60 days after the date of the first benefit payment. Processing option changes may take 30+ days depending on workload constraints. As stated in the audit this may cause the refund distribution of a member's account to span a six month period.

TIME LINE ILLUSTRATION



Benefit due date is the first day of the month following the effective date of retirement

Proposed Corrective Action:

PERS has followed the Audits Division's recommendation to consult with our AG regarding the appropriateness of the lump sum calculation. PERS, in consultation with the AG's office, will evaluate the need to change the interpretation of this statute prospectively to be more consistent with other calculation methods.

Printer Purchase

The audit report concludes that PERS violated its purchasing policy in the purchase of a printer.

Management Response:

PERS agrees.

Proposed Corrective Action:

In response to the audit recommendation that PERS management enforce its purchasing policies, PERS's Director made a presentation on contracting procedures at an agency management meeting. A handout was distributed to managers detailing agency purchasing policy and procedure. The handout contains language extracted from PERS's General Procurement Policy & Procedure and emphasized the necessity for compliance.

Accounts Receivable Management

The audit report concludes that accounts receivable have not been properly managed or supervised.

Management Response:

PERS agrees. The report, however, fails to place this issue in perspective. It is important to understand that Accounts Receivable represent less than .0001 percent of PERS assets and necessarily receives lower priority than other trust accounting activities. PERS recognizes the importance of maintaining appropriate procedures to ensure timely collection of receivables. This is balanced by our desire to be sensitive to our members' needs, as many of these receivables are associated with the death of a PERS retiree and are often due from elderly people on fixed incomes. We strive to be as accommodating as possible, while still carrying out our fiduciary responsibilities.

Corrective Action Proposed:

Relatively recent changes in PERS statutes have allowed PERS to begin collecting outstanding receivables from members receiving annuities by withholding up to 10 percent of their monthly benefit. Consistent with the 1999 Legislature's directive in HB3509, PERS is in the process of closely reviewing outstanding accounts receivable. In addition, we are examining our collection policies and procedures to ensure that we are in compliance with laws and regulations.

**AUDITS DIVISION'S COMMENTS ON THE
AGENCY'S RESPONSE TO THE AUDIT REPORT**

AUDITS DIVISION'S COMMENTS ON THE AGENCY'S RESPONSE TO THE AUDIT REPORT

We have carefully reviewed PERS management's response to the overall findings and recommendations, and the supporting details. Although the agency agreed with the majority of the findings, we found that many of the comments included inaccuracies or misinterpretations of the evidence surrounding the issues included in the report. The following document summarizes the issues related to the various sections of PERS's response:

Comments Relating to the Introduction and Chapter I

We appreciate the agency's concern regarding the cost of the audit. However, PERS management shares in the responsibility for audit costs exceeding original estimates. In many respects, the cost of audits is contingent on factors directly controlled by the agency. These factors include the quality of the agency's policies and procedures, the existence of adequate documentation, and the agency's ability to provide answers to questions. Our initial estimate of audit cost was based on the expectation that PERS Information Technology (IT) processes would be well documented and that we would not encounter major control weaknesses or incidents requiring extensive additional work. As evidenced in the body of our report, this expectation was not realized. Additionally, we expanded our audit to include investigation of several significant issues that came to our attention during the audit, such as those comprising Chapter 4 of this report.

The scope of our audit included objectives to determine whether PERS has sufficient System Development Life Cycle (SDLC) methodologies to maintain its IT applications, including RIMS. During our review, we were surprised to find that the agency lacked well-developed SDLC methodologies. In the later stages of the audit, agency management indicated that they misunderstood our inquiries regarding SDLC. During an audit subcommittee meeting, agency management indicated that they had policies and procedures specific to the OPAS project that they had not revealed to us. We requested to see this information and the subcommittee chair instructed PERS management to furnish it. As a result, they provided some additional information outlining how PERS intended to develop an SDLC methodology for the OPAS system. This information did not contain the expected SDLC methodologies; rather, it was a template for developing them. In a preliminary written response to this audit report, PERS executive director confirmed that the agency's SDLC methodology is a work in process and that it would be developed at a future time.

Our conclusion regarding the risks associated with the OPAS project are based on evidence that the agency continues to lack a comprehensive, well-developed, understood, and utilized SDLC methodology. We have not performed a comprehensive audit of the OPAS project, nor have we made such claims in our report. We do, however, identify that one major key to successful system development and maintenance is missing, a comprehensive SDLC methodology. Given the agency's past

problems developing systems and its ongoing problems maintaining its current system, our conclusions regarding this matter are particularly relevant and timely.

In management's response to Chapter I, PERS states, "In addition, we believe the audit report is incorrect in stating that RIMS does not meet our business needs." However, the agency's statement that only 60 percent of current retirements are processed through RIMS is ample evidence that the system does not meet business needs.

PERS management disagrees with the recommendation to delay development of OPAS until SDLC methodologies are in place. This is an issue where we fundamentally disagree. We believe that the risks associated with developing a major project without a well-developed SDLC far outweigh the risks that may be encountered by delaying the project.

Comments Relating to Chapter II

PERS indicated that having only three individuals with access to modify program code in the production region is unworkable and unreasonable. But every individual given unrestricted, and unmonitored, access to program code increases the risk of introducing unintentional or otherwise unapproved code. We agree that it is sometimes necessary for someone to make direct modifications to code outside of normal business hours to permit processing to continue. Rather than grant additional individuals 24-hour, 7-day access, it is a standard practice to set up a closely-controlled and monitored special ID and password to facilitate such access needs.

PERS also indicates that there are fewer than 80 individuals with the ability to alter programs or data. We reviewed our listing with the PERS security officer who agreed that these individuals had access to change at least one PERS program, or production data set as of the time of our audit. He did indicate that many of these individuals were granted access by mistake, and that he was correcting the problem. Report files are production datasets, and changes to them can have an impact on the agency.

Comments Relating to Chapter III

PERS asserts that the vast majority of its transactions have no problems whatsoever. PERS management also indicates that our sample size was too small to draw any conclusions. Finally, they indicate that they have established effective processing controls and procedures. When reviewing RIMS, we found very few application controls in place; therefore, our conclusions are not based on the transactions we cite, but on the review of PERS controls. The individual examples cited serve to illustrate the types of problems that arise because PERS did not build adequate automated and manual control procedures.

PERS indicates that all of the missing documents cited by our report were either in a working file or were already microfilmed. We did find the two missing manual calculation worksheets in a retirement councilor's files. However, the transaction had

been processed several months prior to our locating these documents, and the documents were subsequently microfilmed once we pointed out the oversight. The other transactions were older, and we reviewed all the microfilmed documents for those members. To date, PERS has not provided us with evidence that these missing documents were microfilmed.

PERS also says that the instances noted were the only duplicate payments found. This is not accurate. The five items cited are the only duplicate payments for which we produced an estimate of lost interest. Our review of PERS's accounts receivable indicated that there have been a number of other duplicate payments that PERS has recovered or is in the process of recovering. PERS's lack of control also would allow other types of duplicate payments to occur.

PERS indicates that the \$94,000 project cleared over 1,800 items and \$77 million in adjustments. During the course of the audit, management was unable to provide us with either a listing or an estimate of the transactions that they cleared during the project. As of October 1999, there were 1,212 items on the out-of-balance listing. Of those, 637 predated September 1998, and 366 were before January 1998. Many transactions on this listing are due to timing differences and will clear on their own. A large number of transactions would have cleared during the project period regardless of PERS efforts. However, approximately half the items listed on the beginning out-of-balance listing were also on the out-of-balance listing when the project ended. Therefore, we believe that PERS's assertions regarding the success of the project may be overstated. PERS's response indicated that a large number of corrections reported by employers inflated the amount on this listing. However, this listing only contains instances when changes to members' reserves did not agree to corresponding changes in benefit reserves.

Comments Relating to Chapter IV

Money Match Lump Sum Benefits

During the audit the Audits Division also consulted with the Attorney General's office. As a result, that office provided PERS and the Audits Division a joint discussion draft covering this issue. Our finding and recommendation is based on our review of that discussion draft in addition to sound accounting practices.

Accounts Receivable Management

PERS indicates that its receivables are .0001 percent of PERS assets. This is true; however, over 99.8 percent of PERS assets are cash, investments, and related receivables managed by the State Treasury and State Street Bank. Of the assets that PERS administers day to day, receivables from employers and members constitute 86 percent; therefore, PERS's implication that this problem is immaterial is inaccurate. This is a legal compliance issue — not an issue of size. Regardless of the balance, PERS has a legal and fiduciary responsibility to collect these amounts.

APPENDIX A

COBIT™ OBJECTIVES RELATING TO SDLC METHODOLOGY

The Information Systems Audit and Control Foundation's Control Objectives for Information and Related Technology (COBIT™) identifies generally accepted and applicable control objectives and practices for information systems. COBIT™ detailed control objectives for SDLC methodologies include, but are not limited to, the following¹:

PO 10.1 Project Management Framework

Control Objective

Management should establish a general project management framework which defines the scope and boundaries of managing projects, as well as the project management methodology to be adopted and applied to each project undertaken. The methodology should cover, at a minimum, allocation of responsibilities, task breakdown, budgeting of time and resources, milestones, check points and approvals.

PO 10.8 System Quality Assurance Plan

Control Objective

Management should ensure that the implementation of a new or modified system includes the preparation of a quality plan which is then integrated with the project master plan and formally reviewed and agreed to by all parties concerned.

PO 10.9 Planning of Assurance Methods

Control Objective

Assurance tasks are to be identified during the planning phase of the project management framework. Assurance tasks should support the accreditation of new or modified systems and should assure that internal controls and security features meet the related requirements.

PO 10.10 Formal Project Risk Management

Control Objective

Management should implement a formal project risk management programme for eliminating or minimising risks associated with individual projects (i.e. identifying and controlling the areas or events that have the potential to cause unwanted change).

¹ COBIT™ Control Objectives, April 1998 2nd Edition

PO 11.4 ***Quality Assurance Review of Adherence to the Information Services Function's Standards and Procedures***

Control Objective

Management should ensure that the responsibilities assigned to the quality assurance personnel include a review of general adherence to the information services function's standards and procedures.

PO 11.5 ***System Development Life Cycle Methodology***

Control Objective

The organisation's senior management should define and implement information systems standards and adopt a system development life cycle methodology governing the process of developing, acquiring, implementing and maintaining computerised information systems and related technology. The chosen system development life cycle methodology should be appropriate for the systems to be developed, acquired, implemented and maintained.

PO 11.6 ***System Development Life Cycle Methodology for Major Changes to Existing Technology***

Control Objective

In the event of major changes to existing technology, management should ensure that a system development life cycle methodology is observed, as in the case of the acquisition of new technology.

PO 11.7 ***Updating of the System Development Life Cycle Methodology***

Control Objective

Senior management should implement a periodic review of its system development life cycle methodology to ensure that its provisions reflect current generally accepted techniques and procedures.

PO 11.10 ***Third Party Implementor Relationships***

Control Objective

Management should implement a process to ensure good working relationships with third-party implementors. Such a process should provide that the user and implementor agree to acceptance criteria, handling of changes, problems during development, user roles, facilities, tools, software, standards and procedures.

PO 11.11 Programme Documentation Standards*Control Objective*

The organisation's system development life cycle methodology should incorporate standards for programme documentation which have been communicated to the concerned staff and enforced. The methodology should ensure that the documentation created during information system development or modification projects conforms to these standards.

PO 11.12 Programme Testing Standards*Control Objective*

The organisation's system development life cycle methodology should provide standards covering test requirements, verification, documentation and retention for testing individual software units and aggregated programmes created as part of every information system development or modification project.

PO 11.13 System Testing Standards*Control Objective*

The organisation's system development life cycle methodology should provide standards covering test requirements, verification, documentation, and retention for the testing of the total system as a part of every information system development or modification project.

PO 11.14 Parallel/Pilot Testing*Control Objective*

The organisation's system development life cycle methodology should define the circumstances under which parallel or pilot testing of new and/or existing systems will be conducted.

PO 11.15 System Testing Documentation*Control Objective*

The organisation's system development life cycle methodology should provide, as part of every information system development, implementation, or modification project, that the documented results of testing the system are retained.

PO 11.16 Quality Assurance Evaluation of Adherence to Development Standards*Control Objective*

The organisation's quality assurance approach should require that a post-implementation review of an operational information system assess whether the

project team adhered to the provisions of the system development life cycle methodology.

AI 1.1 *Definition of Information Requirements*

Control Objective

The organisation's system development life cycle methodology should provide that the business requirements satisfied by the existing system and to be satisfied by the proposed new or modified system (software, data and infrastructure) be clearly defined before a development, implementation or modification project is approved. The system development life cycle methodology should require that the solution's functional and operational requirements be specified including performance, safety, reliability, compatibility, security and legislation.

AI 1.2 *Formulation of Alternative Courses of Action*

Control Objective

The organisation's system development life cycle methodology should provide for the analysis of the alternative courses of action that will satisfy the business requirements established for a proposed new or modified system.

AI 1.3 *Formulation of Acquisition Strategy*

Control Objective

The organisation's system development life cycle methodology should provide for a software acquisition strategy plan defining whether the software will be acquired off-the-shelf, developed internally, through contract or by enhancing the existing software, or a combination of all these.

AI 1.4 *Third-Party Service Requirements*

Control Objective

The organisation's system development life cycle methodology should provide for the evaluation of the requirements and the specifications for an RFP (request for proposal) when dealing with a third-party service vendor.

AI 1.5 *Technological Feasibility Study*

Control Objective

The organisation's system development life cycle methodology should provide for an examination of the technological feasibility of each alternative for satisfying the business requirements established for the development of a proposed new or modified information system project.

AI 1.6 *Economic Feasibility Study*

Control Objective

The organisation's system development life cycle methodology should provide, in each proposed information systems development, implementation and modification project, for an analysis of the costs and benefits associated with each alternative being considered for satisfying the established business requirements.

AI 1.7 *Information Architecture*

Control Objective

Management should ensure that attention is paid to the enterprise data model while solutions are being identified and analysed for feasibility.

AI 1.8 Risk Analysis Report

Control Objective

The organisation's system development life cycle methodology should provide, in each proposed information system development, implementation or modification project, for an analysis and documentation of the security threats, potential vulnerabilities and impacts, and the feasible security and internal control safeguards for reducing or eliminating the identified risk. This should be realised in line with the overall risk assessment framework.

AI 1.9 Cost-Effective Security Controls

Control Objective

Management should ensure that the costs and benefits of security are carefully examined in monetary and non-monetary terms to guarantee that the costs of controls do not exceed benefits. The decision requires formal management sign-off.

AI 1.10 Audit Trails Design

Control Objective

The organisation's system development life cycle methodology should require that adequate mechanisms for audit trails are available or can be developed for the solution identified and selected. The mechanisms should provide the ability to protect sensitive data (e.g. user ID's) against discovery and misuse.

AI 1.11 Ergonomics

Control Objective

Management should ensure that the information system development, implementation and change projects undertaken by the information services function pay attention to ergonomic issues associated with the introduction of automated solutions.

AI 1.12 *Selection of System Software*

Control Objective

Management should ensure that a standard procedure is adhered to by the information services function to identify all potential system software programmes that will satisfy its operational requirements.

AI 1.13 *Procurement Control*

Control Objective

Management should develop and implement a central procurement approach describing a common set of procedures and standards to be followed in the procurement of information technology related hardware, software and services. Products should be reviewed and tested prior to their use and the financial settlement.

AI 1.14 *Software Product Acquisition*

Control Objective

Software product acquisition should follow the organisation's procurement policies.

AI 1.15 *Third-Party Software Maintenance*

Control Objective

Management should require that for licensed software acquired from third-party providers, the providers have appropriate procedures to validate, protect and maintain the software product's integrity rights. Consideration should be given to the support of the product in any maintenance agreement related to the delivered product.

AI 1.16 *Contract Application Programming*

Control Objective

The organisation's system development life cycle methodology should provide that the procurement of contract programming services be justified with a written request for services from a designated member of the information services function. The contract should stipulate that the software, documentation and other deliverables are subject to testing and review prior to acceptance. In addition, it should require that the end products of completed contract programming services be tested and reviewed according to the related standards by the information services function's quality assurance group and other concerned parties (such as users, project managers, etc.) before payment for the work and approval of the end product. Testing to be included in contract specifications should consist of system testing, integration testing, hardware and component testing, procedure testing, load and stress testing, tuning and performance testing, regression testing, user acceptance testing and, finally, pilot testing of the total system to avoid any unexpected system failure.

AI 1.17 *Acceptance of Facilities*

Control Objective

Management should ensure that an acceptance plan for facilities to be provided is agreed upon with the supplier in the contract and this plan defines the acceptance procedures and criteria. In addition, acceptance tests should be performed to guarantee that the accommodation and environment meet the requirements specified in the contract.

AI 1.18 *Acceptance of Technology*

Control Objective

Management should ensure that an acceptance plan for specific technology to be provided is agreed upon with the supplier in the contract and this plan defines the acceptance procedures and criteria. In addition, acceptance tests provided for in the plan should include inspection, functionality tests and workload trials.

AI 2.1 *Design Methods*

Control Objective

The organisation's system development life cycle methodology should provide that appropriate procedures and techniques, involving close liaison with system users, are applied to create the design specifications for each new information system development project and to verify the design specifications against the user requirements.

AI 2.2 *Major Changes to Existing Systems*

Control Objective

Management should ensure, that in the event of major changes to existing systems, a similar development process is observed as in the case of the development of new systems.

AI 2.3 *Design Approval*

Control Objective

The organisation's system development life cycle methodology should require that the design specifications for all information system development and modification projects be reviewed and approved by management, the affected user departments and the organisation's senior management, when appropriate.

AI 2.4 *File Requirements Definition and Documentation*

Control Objective

The organisation's system development life cycle methodology should provide that an appropriate procedure be applied for defining and documenting the file format for each information system development or modification project. Such a procedure should ensure that the data dictionary rules are respected.

AI 2.5 *Programme Specifications*

Control Objective

The organisation's system development life cycle methodology should require that detailed written programme specifications be prepared for each information system development or modification project. The methodology should further ensure that programme specifications agree with system design specifications.

AI 2.6 *Source Data Collection Design*

Control Objective

The organisation's system development life cycle methodology should require that adequate mechanisms for the collection and entry of data be specified for each information system development or modification project.

AI 2.7 *Input Requirements Definition and Documentation*

Control Objective

The organisation's system development life cycle methodology should require that adequate mechanisms exist for defining and documenting the input requirements for each information system development or modification project.

AI 2.8 *Definition of Interfaces*

Control Objective

The organisation's system development life cycle methodology should provide that all external and internal interfaces are properly specified, designed and documented.

AI 2.9 *User-Machine Interface*

Control Objective

The organisation's system development life cycle methodology should provide for the development of an interface between the user and machine which is easy to use and self-documenting (by means of online help functions).

AI 2.10 *Processing Requirements Definition and Documentation*

Control Objective

The organisation's system development life cycle methodology should require that adequate mechanisms exist for defining and documenting the processing requirements for each information system development or modification project.

AI 2.11 *Output Requirements Definition and Documentation*

Control Objective

The organisation's system development life cycle methodology should require that adequate mechanisms exist for defining and documenting the output requirements for each information system development or modification project.

AI 2.12 *Controllability*

Control Objective

The organisation's system development life cycle methodology should require that adequate mechanisms for assuring the internal control and security requirements be specified

for each information system development or modification project. The methodology should further ensure that information systems are designed to include application controls which guarantee the accuracy, completeness, timeliness and authorisation of inputs, processing and outputs. Sensitivity assessment should be performed during initiation of system development or modification. The basic security and internal control aspects of a system to be developed or modified should be assessed along with the conceptual design of the system in order to integrate security concepts in the design as early as possible.

AI 2.13 *Availability as a Key Design Factor*

Control Objective

The organisation's system development life cycle methodology should provide that availability is considered in the design process for new or modified information systems at the earliest possible stage. Availability should be analysed and, if necessary, increased through maintainability and reliability improvements.

AI 2.14 *Information Technology Integrity Provisions in Application Programme Software*

Control Objective

The organisation should establish procedures to assure, where applicable, that application programmes contain provisions which routinely verify the tasks performed by the software to help assure data integrity, and which provide in the restoration of the integrity through rollback or other means.

AI 2.15 *Application Software Testing*

Control Objective

Unit testing, application testing, integration testing, system testing, and load and stress testing should be performed according to the project test plan and established testing standards before it is approved by the user. Adequate measures should be conducted to prevent disclosure of sensitive information used during testing.

AI 2.16 User Reference and Support Materials

Control Objective

The organisation's system development life cycle methodology should provide that adequate user reference and support manuals be prepared (preferably in electronic format) as part of every information system development or modification project.

AI 2.17 Re-Assessment of System Design

Control Objective

The organisation's system development life cycle methodology should ensure that the system design is re-assessed whenever significant technical and/or logical discrepancies occur during system development or maintenance.

AI 3.1 Assessment of New Hardware and Software

Control Objective

Procedures should be in place to assess new hardware and software for any impact on the performance of the overall system.

AI 3.2 Preventative Maintenance for Hardware

Control Objective

Management of the information services function should schedule routine and periodic hardware maintenance to reduce the frequency and impact of performance failures.

AI 3.3 System Software Security

Control Objective

Management of the information services function should ensure that the set-up of system software to be installed does not jeopardise the security of the data and programmes being stored

on the system. Attention should be paid to set-up and maintenance of system software parameters.

AI 3.4 *System Software Installation*

Control Objective

Procedures should be implemented to ensure that system software is installed in accordance with the acquisition and maintenance framework for the technology infrastructure. Testing should be performed before use in the production environment is authorised.

AI 3.5 *System Software Maintenance*

Control Objective

Procedures should be implemented to ensure that system software is maintained in accordance with the acquisition and maintenance framework for the technology infrastructure.

AI 3.6 *System Software Change Controls*

Control Objective

Procedures should be implemented to ensure that system software changes are controlled in line with the organisation's change management procedures.

AI 4.1 *Future Operational Requirements and Service Levels*

Control Objective

The organisation's system development life cycle methodology should ensure the timely definition of future operational requirements and service levels.

AI 4.2 *User Procedures Manuals*

Control Objective

The organisation's system development life cycle methodology should provide that adequate user procedures manuals be prepared and refreshed as part of every information system development, implementation or modification project.

AI 4.3 *Operations Manual*

Control Objective

The organisation's system development life cycle methodology should provide that an adequate operations manual be prepared and kept up-to-date as part of every information system development, implementation or modification project.

AI 4.4 *Training Materials*

Control Objective

The organisation's system development life cycle methodology should assure that adequate training materials are developed as part of every information system development, implementation or modification project. These materials should be focused on the system's use in daily practice.

AI 5.1 *Training*

Control Objective

Staff of the affected user departments and the operations group of the information services function should be trained in accordance with the defined training plan and associated materials, as part of every information systems development, implementation or modification project.

AI 5.2 *Application Software Performance Sizing*

Control Objective

Application software performance sizing (optimisation) should be established as an integral part of the organisation's system development life cycle methodology to forecast the resources required for operating new and significantly changed software.

AI 5.3 *Conversion*

Control Objective

The organisation's system development life cycle methodology should provide, as part of every information system development, implementation or modification project, that the necessary elements from the old system are converted to the new one according to a pre-established plan.

AI 5.4 *Testing of Changes*

Control Objective

Management should ensure that changes are tested in accordance with the impact and resource assessment in a separate test environment by an independent (from builders) test group before use in the regular operational environment begins. Back-out plans should also be developed. Acceptance testing should be carried out in an environment representative of the future operational environment (e.g. similar security, internal controls, workloads, etc.).

AI 5.5 *Parallel / Pilot Testing Criteria and Performance*

Control Objective

Procedures should be in place to ensure that parallel or pilot testing is performed in accordance with a pre-established plan and that the criteria for terminating the testing process are specified in advance.

AI 5.6 Final Acceptance Test

Control Objective

Procedures should provide, as part of the final acceptance or quality assurance testing of new or modified information systems, for a formal evaluation and approval of the test results by management of the affected user department(s) and the information services function. The tests should cover all components of the information system (e.g. application software, facilities, technology, user procedures).

AI 5.7 Security Testing and Accreditation

Control Objective

Management should define and implement procedures to ensure that operations and user management formally accept the test results and the level of security for the systems, along with the remaining residual risk.

AI 5.8 Operational Test

Control Objective

Management should ensure that before moving the system into operation, the user or designated custodian (the party designated to run the system on behalf of the user) validates its operation as a complete product, under conditions similar to the application environment and in the manner in which the system will be run in a production environment.

AI 5.9 Promotion to Production

Control Objective

Management should define and implement formal procedures to control the handover of the system from development to testing to operations. The respective environments should be segregated and properly protected.

AI 5.10 *Evaluation of Meeting User Requirements*

Control Objective

The organisation's system development life cycle methodology should require that a post-implementation review of operational information system requirements (e.g. capacity, throughput, etc.) be conducted to assess whether the users' needs are being achieved by the system.

AI 5.11 *Management's Post-Implementation Review*

Control Objective

The organisation's system development life cycle methodology should require that a post-implementation review of an operational information system assess and report on whether the system delivered the benefits envisioned in the most cost effective manner.

AI 6.1 *Change Request Initiation and Control*

Control Objective

Management should ensure that all requests for changes, system maintenance and supplier maintenance are standardised and are subject to formal change management procedures. Changes should be categorised and prioritised and specific procedures should be in place to handle urgent matters. Change requestors should be kept informed about the status of their request.

AI 6.2 *Impact Assessment*

Control Objective

A procedure should be in place to ensure that all requests for change are assessed in a structured way for all possible impacts on the operational system and its functionality.

AI 6.3 *Control of Changes*

Control Objective

Management should ensure that change management, and software control and distribution are properly integrated with a comprehensive configuration management system.

AI 6.4 *Documentation and Procedures*

Control Objective

The change process should ensure that whenever system changes are implemented, the associated documentation and procedures are updated accordingly.

AI 6.5 *Authorised Maintenance*

Control Objective

Management should ensure maintenance personnel have specific assignments and that their work is properly monitored. In addition, their system access rights should be controlled to avoid risks of unauthorised access to automated systems.

AI 6.6 *Software Release Policy*

Control Objective

Management should ensure that the release of software is governed by formal procedures ensuring sign-off, packaging, regression testing, handover, etc.

AI 6.7 ***Distribution of Software***

Control Objective

Specific internal control measures should be established to ensure distribution of the correct software element to the right place, with integrity, and in a timely manner with adequate audit trails.

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/audithp.htm>

Auditing to Protect the Public Interest and Improve Oregon Government