

---

Secretary of State

State of Oregon

**DEPARTMENT OF ADMINISTRATIVE SERVICES**

**Oregon State Payroll System**

Application Control Review



Audits Division

---



---

Secretary of State

State of Oregon

**DEPARTMENT OF ADMINISTRATIVE SERVICES**

**Oregon State Payroll System**

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

Michael Greenfield, Director  
Department of Administrative Services  
155 Cottage Street NE  
Salem, Oregon 97310

This report includes an evaluation of the computer application controls governing the Oregon State Payroll System (OSPS). Application controls relate to specific processing requirements to ensure that data remains complete, accurate, and valid during input, processing, and output.

During this audit, we reviewed control procedures in operation between March and July 1999, including procedures to manage changes to the system and manage data during its input, processing and output. We also reviewed the organizational structure of OSPS and procedures to ensure system security.

Our report includes recommendations to improve management of the Oregon State Payroll System. The Department of Administrative Services generally agrees with our recommendations.

OREGON AUDITS DIVISION

John N. Lattimer  
Director

Fieldwork Completion Date:  
July 16, 1999



# TABLE OF CONTENTS

	<u>Page</u>
SUMMARY .....	vii
INTRODUCTION.....	1
Information System Controls .....	1
Scope and Methodology.....	2
AUDIT RESULTS	
Managing Change .....	3
Managing Data .....	5
Data Processing Validation and Editing.....	5
Backup and Offsite Storage .....	6
Organizational Structure .....	6
Ensuring System Security .....	7
Special Access.....	7
Dual Access .....	8
Matter For Consideration .....	10
COMMENDATION .....	11
AGENCY'S RESPONSE TO THE AUDIT REPORT .....	13



## SUMMARY

### BACKGROUND

The Oregon State Payroll System (OSPS) operates within the Department of Administrative Services (DAS) State Controller's Division. OSPS is the central payroll system, processing payroll for approximately 34,000 state employees per month. Total expenditures processed through OSPS exceed \$1 billion per year.

### AUDIT PURPOSE

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

### AUDIT RESULTS

DAS should consider the following priority items to improve its controls governing OSPS:

- Ensure that programming changes made to the system follow a comprehensive System Development Life Cycle (SDLC) methodology.
- Identify, document and review OSPS edits to ensure that they are effective.
- Assign responsibility for the management of OSPS backup and offsite storage. In addition, the OSPS manager should provide specific direction to IRMD regarding its role, including regular periodic reviews of which data should be stored offsite.
- Assign check reconciliation duties to employees who are independent of the manual check writing process. The OSPS manager should also more closely monitor the manual check function.
- Review and adjust access granted to programmers and Central Payroll to ensure that it is based on the individual's demonstrated need to view, add, change or delete data.
- Develop procedures to closely monitor programmers' emergency access to production libraries.

- Comply with existing DAS policy regarding monitoring dual access. DAS also should clarify its policy to specify who is responsible for monitoring this access.
- Comply with Oregon State Treasury policies and procedures regarding control of blank check stock.

**AGENCY'S RESPONSE** The Department of Administrative Services generally agrees with our recommendations.

## **INTRODUCTION**

The Department of Administrative Services (DAS) State Controller's Division operates the Oregon State Payroll System (OSPS). OSPS is the centralized statewide payroll system, processing payroll checks and direct deposit payments for over 34,000 state employees each month. In addition, it provides necessary reporting, vendor payments, and federal and state tax deposits for more than 100 state agencies. Total payroll expenditures processed through OSPS exceed \$1 billion per year.

OSPS interfaces with other statewide computer systems, including the Position Personnel Data Base (PPDB), the Statewide Financial Management System (SFMS), and various applications at the Oregon State Treasury. From the PPDB, OSPS receives specific information necessary to process payroll. In turn, OSPS provides SFMS payroll accounting information. Finally, OSPS provides the Oregon State Treasury daily files of checks created through the system.

OSPS is maintained by Support Services (Central Payroll), which includes a manager and four staff members. In addition, the DAS Information Resources Management Division (IRMD) provides additional technical services to help maintain OSPS. IRMD has four staff members that provide programming, systems analysis, project management, and database administration services to OSPS and other systems. This staff includes a manager, system supervisor, senior analyst and programmer. IRMD also provides backup and processing services for the system.

## **INFORMATION SYSTEM CONTROLS**

Information system controls are generally classified as either application controls or general controls. Application controls relate to specific processing requirements to ensure data remains complete, accurate, and valid during input, processing, and output. These controls are designed to reduce errors that may occur during the operation of an individual system, application or program. General controls are intended to protect the environment in which computer systems process. These controls focus on physical security, access controls, backup and restoration, segregation of duties, and appropriate operation and maintenance of the system.

Application controls coupled with general controls provide assurance that authorized transactions processed through the system are complete and reliable. Central Payroll and IRMD are responsible for providing adequate general and application controls to reduce the risk of errors in the system's operation.

## **SCOPE AND METHODOLOGY**

This audit reviewed the OSPS application controls. We performed our fieldwork between March and July 1999. The audit included a review of the control procedures operating during the specified time period for the following control areas:

- Managing Change
- Managing Data
- Organizational Structure
- Ensuring System Security

The objective of our audit was to evaluate the adequacy of application controls established for OSPS as of March 1999. We made inquiries of OSPS, the State Controller's Division, and IRMD personnel; examined documentation supporting controls and procedures; and observed OSPS control processes and operations. We evaluated compliance with applicable laws, rules and regulations pertaining to internal control and the operation of OSPS. During our audit we used the Information Systems Audit and Control Foundation's (ISACF) document "Control Objectives for Information and Related Technology" (CobiT) to identify generally accepted and applicable internal control objectives and practices. ISACF is a worldwide organization dedicated to research, develop, and publicize generally accepted information technology control objectives and audit guidelines.

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

## AUDIT RESULTS

### MANAGING CHANGE

Oregon State Payroll System (OSPS) Support Services (Central Payroll) is responsible for ensuring that OSPS functions to meet user needs and requirements. To meet those changing needs, Central Payroll relies on the Department of Administrative Services (DAS) Information Resources Management Division (IRMD) Systems Development and Consulting Section to perform the necessary programming changes.

Programming changes should be made using a written systematic approach to ensure that all requirements are met and that only authorized changes occur. Controls to manage those changes should be established to minimize the likelihood that disruptions, unauthorized alterations, or errors could be introduced into the system. This approach to making programming changes is called System Development Life Cycle (SDLC) methodology. The SDLC methodology includes change management procedures for ongoing system maintenance as well as new system development.

IRMD has a written SDLC methodology for maintaining OSPS. This methodology requires certain steps be completed when performing minor projects or system enhancements. The IRMD System Development Manager (IRMD manager) is responsible for ensuring that programmers working on OSPS follow the methodology. In turn, the OSPS manager is ultimately responsible for ensuring that IRMD follows the written methodology.

IRMD's SDLC methodology provides some of the controls necessary to ensure that changes meet users' needs and data integrity is maintained. The methodology, however, does not provide assurance that requests are initiated through the proper means and appropriately tracked and authorized. Central Payroll has not developed procedures to address this deficiency.

Additionally, IRMD does not follow its SDLC methodology, nor does the OSPS manager ensure that IRMD follows the methodology. We noted the following concerns:

- The IRMD programmers' documentation of work performed on system design and program testing is inadequate. For example, the programmers' design notes and results of tests generally are not retained. In addition, they do not always update system manuals to reflect the changes that they made to the system.
- The OSPS manager does not ensure that all program changes are tested and does not review testing results. Also, end-user acceptance testing does not occur for all changes.
- Central Payroll does not review general and detailed designs of the programming changes to be made.
- The IRMD manager does not effectively monitor program changes performed by her staff. Rather, she approves programming changes without reviewing evidence that the programmers complied with the required SDLC methodology and that no unauthorized code was introduced.

These conditions exist because the OSPS manager does not ensure that changes made to the system follow an established SDLC methodology. She relies on IRMD to follow its methodology. Since IRMD does not fully comply with its SDLC methodology, there is an increased likelihood that disruptions, unauthorized alterations, and errors could occur.

**We recommend** that the OSPS manager ensure that changes made to the system follow a comprehensive SDLC methodology. This methodology should ensure that system change requests are properly initiated, tracked and authorized. We also recommend that the OSPS manager take a more active role to ensure that IRMD follows the established methodology.

## MANAGING DATA

Controls to manage data help to ensure data remains accurate, valid and complete during input, processing, output and storage. These controls include data processing validation and editing routines as well as procedures to control backup and offsite storage.

Data processing validation and editing routines include system edits to prevent erroneous data from being entered into the system. They also include programmed edits to detect data errors so that they may be corrected or excluded from processing. These system edits should be tested after programming changes to ensure that they remain valid and effective.

Backup and offsite storage procedures should ensure that the operating data and programs can be restored to the system in the event of a disaster. These controls include routinely backing up all necessary files and storing them in a secure offsite location.

### **Data Processing Validation and Editing**

IRMD programmers and the OSPS manager were unable to readily identify all existing OSPS system edits. In addition, they do not always review or test system edits to ensure they are effective or valid after making programming changes to OSPS.

Their inability to identify system edits and subsequently review and test them is the result of inadequate program documentation.

This lack of documentation and regular review and testing of system edits increases the risk that these routines may be ineffective or invalid. Existing edits may contain errors or their parameters may be inappropriately set, thus limiting their ability to function as intended. This condition increases the likelihood that OSPS may accept and process invalid data.

**We recommend** that IRMD programmers identify, document and review system edits to ensure that they are effective. In addition, the OSPS manager should periodically review these edits to ensure they remain appropriate.

## **Backup and Offsite Storage**

The DAS General Government Data Center (GGDC) backs up OSPS files according to a schedule created in 1995; however, the OSPS manager does not ensure that backup and offsite storage is sufficient and that it occurs on a regular basis. For example, neither the OSPS manager nor the IRMD programmers are certain which files should be backed up or stored offsite, or which files should be restored in the event of a disaster.

This condition exists because these backup duties have not been specifically assigned to either the OSPS manager or the IRMD programmer. Thus, neither monitors GGDC personnel to ensure that backups include all the necessary files. As a result, GGDC may not have all the required tapes stored in its designated offsite location to restore the system in the event of a disaster or other disruption.

**We recommend** that DAS specifically assign responsibility for the management of OSPS backup and offsite storage. In addition, we recommend the OSPS manager provide specific direction to IRMD regarding its role, including regular periodic reviews of which data should be stored offsite.

## **ORGANIZATIONAL STRUCTURE**

Management should implement a division of roles and responsibilities that minimizes the possibility that a single individual could undermine a critical process. Management should also ensure that personnel perform only those duties included in their respective jobs and positions.

One critical function of Central Payroll is to prepare manual checks twice daily. These checks are prepared in addition to the regular bimonthly payroll, and result from employee terminations, payroll corrections and adjustments, and payroll advances. During this process, Central Payroll employees share duties that should be separated to provide adequate internal control. These internal control weaknesses include the following:

- The OSPS manager has not provided appropriate restrictions on Central Payroll employees' access to

input screens, printer fonts, and blank check stock used to print manual checks.

- The staff member primarily responsible for verifying the manual checks also serves as the designated backup for writing manual checks.
- A person independent of the manual check function does not review the checks prior to distribution, or review the manual check verification to ensure all items are properly supported.

Inadequate segregation of duties is an organizational problem. Position descriptions for three of five Central Payroll staff list both the manual check processing and manual check verification as required job duties. The position description of the OSPS manager does not specify her responsibility to monitor the work of Central Payroll. As a result of inadequate segregation and supervision of duties, a single employee could subvert the manual check process.

**We recommend** that DAS management assign check reconciliation duties to employees who are independent of the manual check writing process. We also recommend that the OSPS manager more closely monitor the manual check function.

## **ENSURING SYSTEM SECURITY**

### **Special Access**

Access to the system should be provided according to an individual's demonstrated need to view, add, change, or delete data. The OSPS manager is ultimately responsible for ensuring security for the system by providing appropriate access controls. These controls should ensure that employees who maintain and operate the system have only those access privileges needed to perform their duties.

IRMD programmers assigned to OSPS perform program changes and should not perform any additional system or user functions. Therefore, their access should be restricted to the test region where they perform their work. However, when problems occur during production,

they may need access to the production region to perform emergency system maintenance. Under these circumstances, their access and work should be closely monitored.

Central Payroll employees perform various functions such as creating manual checks, making special adjustments, and assisting end-users. Accordingly, their access should be restricted to allow them to perform only their assigned duties.

The State Controller's Division does not always grant access to OSPS based on users' demonstrated need to view, add, change or delete data. Programmers have unlimited and unsupervised access to the production region. In addition, Central Payroll employees have update access to various OSPS screens that they do not need to perform their duties. For example, staff members have update access to time entry screens even though they do not perform this function. Also, the OSPS manager has unneeded update access to the time entry and manual check screens.

Programmers having access beyond their need increases the risk that unintended code may be introduced into the system. In addition, it increases the risk that programmers could bypass controls intended to protect the integrity of the data and system. Furthermore, Central Payroll employees having greater access than what they need increases the risk that fraudulent or erroneous transactions may occur and go undetected.

### **Dual Access**

The Position Personnel Data Base (PPDB) interfaces with OSPS, providing information needed to process payroll. Update access to PPDB allows users to input new or modify existing employees' records. Because OSPS and PPDB functions should be separated to provide adequate control, DAS management should closely monitor users having update access to both systems.

The PPDB manager is responsible for controlling user access to PPDB. In certain, limited situations some users require both PPDB and OSPS access. To compensate for dual access to the PPDB and OSPS systems, DAS has developed policies and procedures to mitigate some of the

associated risks. Its policy requires dual-access users to obtain written approval from both the PPDB and OSPS managers. It also requires a monthly review of access privileges to ensure that only authorized employees have dual access.

We found that DAS management does not sufficiently monitor dual access. For example, the security administrator did not retain approval letters to document all dual access granted, and monthly access reviews were not conducted by the security administrator or the PPDB manager. Monthly reviews were not conducted, in part, because DAS policy does not specify who should perform the reviews.

By not adequately monitoring dual access to OSPS and PPDB, the risk is greater that inappropriate or fraudulent transactions may occur and go undetected. At this time, we did not test transactions initiated by individuals having dual access.

**We recommend** that the OSPS manager review access granted to IRMD programmers and Central Payroll employees to ensure that this access is based on each individual's demonstrated need to view, add, change or delete data. In addition, we recommend that the OSPS manager and the IRMD manager develop procedures to further limit programmers' access to production libraries. Programmers' access to production libraries only should be granted to accommodate emergencies. In these special instances, we recommend that the IRMD manager closely monitor the programmers' activities.

**We also recommend** that the OSPS manager and the PPDB manager comply with existing DAS policy regarding monitoring dual access. DAS also should clarify its policy to specify who is responsible for performing the monthly reviews.

**MATTER FOR  
CONSIDERATION**

Although not included in our original scope, during the course of our audit procedures we noted that Central Payroll was not fully complying with the Oregon State Treasury's policies and procedures to control check stock. Specific noncompliance to these policies and procedures includes the following:

- Access to check stock has not been restricted.
- Check stock remains unsecured during the day.
- There is no physical inventory of blank check stock and blank check stock is not tracked.
- There are no procedures for defacing/retaining voided checks.
- Controls over printer fonts required to print checks are inadequate.

With the single state check stock being used by all agencies, inadequate physical controls over blank check stock at any one agency increase the likelihood of fraud throughout the state. Without proper controls, the risk of checks being stolen or fraudulently used increases significantly. This risk increases when combined with a lack of appropriate segregation of duties within Central Payroll.

**We recommend** that Central Payroll comply with the Oregon State Treasury's policies and procedures regarding physical access to blank check stock. The OSPS manager should assign a staff member to this process to ensure that it occurs. We also recommend that the DAS Internal Audit section periodically monitor controls over blank check stock to ensure adherence to those policies and procedures.

## **COMMENDATION**

The courtesies and cooperation extended by officials and employees of the Department of Administrative Services during the course of this review were commendable and sincerely appreciated.

## **AUDIT TEAM**

Neal E. Weatherspoon, CPA, CISA, Audit Administrator  
Janice I. Richards, CPA  
Shandi C. Maxwell



**AGENCY'S RESPONSE TO THE AUDIT REPORT**





# Oregon

John A. Kitzhaber, M.D., Governor

Department of Administrative Services

Office of the Director  
155 Cottage Street NE  
Salem, OR 97310-0310  
(503) 378-3104  
FAX (503) 373-7643

## MEMORANDUM

Date: March 6, 2000

To: John Lattimer, Director  
Audits Division, Secretary of State

From:   
Michael Greenfield, Director  
Department of Administrative Services

Subject: Response to Draft Audit Report

Thank you for the opportunity to comment on your draft audit report on the Application Control Review of the Oregon State Payroll System.

Recommendation:

**System programming changes: Ensure changes follow comprehensive System Development Life Cycle methodology.**

Response:

We agree. By March 2000, OSPS will develop procedures to document that change requests are appropriately tracked and authorized. We will use a database tracking system with IRMD to jointly track changes, testing and results and authorizations to move to production. Additionally, we will update our Service Level Agreement with IRMD to more clearly define responsibilities. The OSPS manager is responsible for this item.

Recommendation:

**Data Processing Validation and Editing: Identify, document and review system edits to ensure they are effective, and periodically review these edits to ensure they remain appropriate.**

Response:

We agree. Documentation exists for the original system requirements, but has not been consistently updated because of resource limitations. All production on-line and batch programs have been identified. The OSPS manager and IRMD systems supervisor expect to develop a plan with timelines and procedures for integrating original requirements with current system edits, focusing initially on the critical area of on-line processing by June 2000. Progress will be reviewed quarterly by the OSPS Manager and IRMD Systems Supervisor. Once completed, the edits will be reviewed annually by the OSPS manager. The IRMD SD&C manager is responsible for this item.



John Lattimer  
March 6, 2000

Recommendation:

**Backup and Offsite Storage: Assign specific responsibility for management of OSPS backup and offsite storage. The OSPS manager should provide specific direction to IRMD regarding its role, including regular periodic reviews of which data should be stored offsite.**

Response:

We partially agree. DAS has assigned specific responsibility for OSPS backup and offsite storage to the IRMD OSPS Systems Supervisor. Backup and offsite storage does occur on a weekly basis. IRMD expects to review and update the backup and offsite storage plan for OSPS by June 2000. We will identify which files should be backed up and stored offsite and which files should be restored in the event of a disaster. Periodic reviews of the updated plan involving the OSPS manager and IRMD will coincide with testing of the IRMD General Government Data Center (GGDC) disaster recovery plan. The IRMD SD&C manager is responsible for this item.

Recommendation:

**Check reconciliation duties: Assign duties to employees who are independent of the manual check writing process. More closely monitor the manual check function.**

Response:

We agree. Effective 3/1/00 we will reassign the task of manual check reconciliation to an accountant in the Statewide Accounting and Reporting Section (SARS). The OSPS manager will review the completed reconciliation.

We will reduce the check font downloading capability to only the position that has primary responsibility for the manual check process. As a backup, to ensure functionality, check font downloading will be possible from the computer of the OSPS manager, who will have no ability to produce a manual check.

The OSPS Manager or other SCD management employee will conduct a high-level review of manual checks. In addition, DAS Internal Audit will use random sampling to audit manual check activity twice a year. Another mitigating control to consider is that the receiving payroll office reviews the manual check outputs for accuracy and compliance with initial payroll requests.

Recommendation:

**Ensuring system security – Special access: Review on-line data access to assure appropriate use. Develop procedures to further limit programmers' access to production libraries. Monitor programmer activities to perform emergency system maintenance.**

Response:

We partially agree. On-line production access is controlled centrally through security tables. Screen update activity is monitored through reports provided to the OSPS manager after each payroll processing. However, OSPS will reevaluate access granted to IRMD programmers and Central Payroll employees by June 2000 to ensure that access is based on each individual's demonstrated need to view, add, change or delete data.

John Lattimer  
March 6, 2000

The OSPS Manager is advised, and approves, of emergency system maintenance as it arises. However, separate RACF IDs will be implemented as soon as possible to limit and monitor programmers' access to production libraries. These RACF IDs will be used only for job monitoring, and off-hour support such as responding to abends, which require production authority. IRMD Systems Development and Consulting will work with the IRMD General Government Data Center and the DAS Internal Auditor to develop a report and procedure to provide for the routine monitoring of this activity. We expect to implement the reporting and monitoring process no later than June 2000. The OSPS Manager will ensure this work is completed on time.

Recommendation:

**Ensuring system security – Special access: Review central payroll's on-line data access to assure appropriate use. Comply with DAS policy regarding dual access to OSPS and PPDB.**

Response:

We agree. We will analyze the access of each central payroll staff member and reduce update access to only those areas of the system that are absolutely necessary for performance of duties and maintenance of customer service levels. We will work with SCD Security to carry out the plan and we will adequately document the plan. This will be completed no later than 3/31/00. The OSPS Manager will be responsible for this item.

The OSPS manager will work with the PPDB manager to analyze current dual access and develop a plan and procedure to perform a monthly review. This will be completed no later than 3/31/00. In addition, the SCD will work with the agencies involved to eliminate dual access if possible.

Recommendation:

**Comply with the Oregon State Treasury's policies and procedures: control access to and inventory blank check stock, retain all voided checks and control font access.**

Response:

We agree. We will immediately strengthen controls over access to blank check stock. By April 2000 we will be in complete compliance with Treasury's policies and procedures. We will retain all voided checks rather than the samples and explanations presently retained. The OSPS manager is responsible for this item.

Thank you for your comments on matters noted during your audit of the Oregon State Payroll System Application Review. If you have any questions or need additional information, please call Valerie Wicklund at 378-3742.



## **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](mailto:Audits.Hotline@state.or.us)

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

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