



# Secretary of State Audit Report

## Oregon Department of Human Services: Combined Check Reconciliation System & Accounting Interface Application Controls Review

### Summary

#### PURPOSE

The purpose of this audit was to evaluate the effectiveness of key general and application computer controls relating to the Oregon Department of Human Services' (department) Combined Check Reconciliation System & Accounting Interface (system). Our specific audit objectives were to determine whether the department implemented processes to reasonably ensure system data integrity, backup and recovery, program change management, and logical access control.

#### RESULTS IN BRIEF

In general, the department's application controls provided reasonable assurance that most data would remain complete, accurate and valid during system input, processing and output. However, those controls were not as effective for manually adjusted transactions. Control weaknesses relating to these adjustments increased the likelihood that inappropriate or erroneous information could be entered into the system and transferred to the state's accounting system.

It was also unlikely the department could timely, or fully, restore system information from off-site backup tapes because some critical system files were not appropriately backed up to tape and because the department lacked a defined and tested recovery plan.

We also found that program change management controls did not always follow generally accepted control practices. Specifically, technical reviews of modified code were not always performed, approved code changes were not adequately safeguarded, and certain production data sets were directly modified by staff.

In addition, logical access controls did not adequately protect the system and its data. Because of the sensitive nature of system security, we issued a separate management letter outlining specific details of our findings, as well as recommendations to improve security.

That confidential letter was prepared in accordance with ORS 192.501 (23), which exempts such information from public disclosure.

#### RECOMMENDATIONS

To resolve these issues, we recommend that department management:

- develop and implement policies and procedures to ensure all changes to system data are appropriately reviewed and approved before they are transmitted to SFMA;
- formally assign responsibility for timely resolving problems identified in all system error reports, consider making system modifications to enhance audit trail information, and ensure identified system reporting issues are resolved;
- develop, implement, and test strategies to ensure backups of all critical files are performed and stored off-site and specific backup and recovery roles and responsibilities are defined, assigned and formally coordinated with the State Data Center via a written service level agreement;
- develop more robust program change management policies and procedures to require independent technical reviews of code modifications, more restrictive logical access control of approved code prior to approval and elevation to production, and the use of a controlled environment outside of production for routine data set modifications;
- consider using software code-compare utilities; and
- implement the recommendations included in our confidential management letter.

#### AGENCY'S RESPONSE

The Department of Human Services agrees with the recommendations.

## Background

The Oregon Department of Human Services (department) is responsible for administering numerous programs that provide assistance to qualified persons in need. The department utilizes various automated computer applications to help administer these programs and provide payments to individuals or their providers.

To account for all expenditures made through its various payment systems, the department uses the state's centralized Statewide Financial Management Application (SFMA). To automate SFMA input and to track the status of checks written by most department payment systems, the department developed and implemented the Accounting Interface (AI) and Combined Check Reconciliation System (CCRS) computer applications.

During 2003, the department began a project to combine and improve the functionality of AI and CCRS. In September 2006, it moved the first version of the combined system into production.

From September to October 2006, the Combined Check Reconciliation System & Accounting Interface (system) processed approximately \$235 million in check and electronic funds transfers each month. Department employees use system inquiry screens and reports to determine the current status of individual checks and to facilitate reconciliations of the department's Treasury and SFMA cash accounts. Nearly all transactions flow through the system automatically.

The system is maintained by department personnel and hosted on a Department of Administrative Services' mainframe computer at the State Data Center.

## Audit Objectives

The purpose of this audit was to evaluate the effectiveness of key general and application computer controls relating to the department's Combined Check Reconciliation System & Accounting Interface.

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

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

## Audit Results

### Manual Data Adjustments Were Not Always Adequately Controlled

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

During our audit, we performed various tests of system data to determine the effectiveness of manual and automated application controls. Based on the results of these tests, we concluded that controls were adequate to ensure:

- system tables were appropriately updated to reflect check issuance data;
- check and electronic funds transfer information sent from source systems were received completely;
- transactions were summarized for submission to SFMA; and
- all transactions sent from the system were received by SFMA.

For the period we tested, all transactions flowed through the system as described above. However, approximately two percent of checks recorded in the system were subsequently adjusted to correct a variety of data errors and discrepancies, or to update their status when they were cancelled. We noted the following control weaknesses relating to these manual adjustment processes:

- Adjusting entries were not always reviewed and approved prior to processing.
- Data discrepancies identified in some error reports were not always timely or appropriately resolved.
- Reconciliation reports did not always accurately reflect the results of some adjustments. Specifically, some beginning report balances did not agree with prior ending balances.
- Audit trails did not provide complete history of all adjustments made to check information.

These control weaknesses increased the likelihood that inappropriate transactions or erroneous information could be manually entered into the system and subsequently transferred to SFMA via the interface.

We noted that department management had not developed or implemented policies or procedures

requiring review and approval of system adjusting entries. In addition, managers had not formally assigned responsibility for resolving all system error reports. Furthermore, we concluded that report integrity issues and insufficient audit trails were the result of the department's system design decisions.

**We recommend** that department management develop and implement policies and procedures to ensure all changes to system data are appropriately reviewed and approved before they are transmitted to SFMA.

***Agency's Response:***

*The department agrees with this recommendation. The department will develop procedures requiring the review and approval of system adjusting entries before they are transmitted to SFMA. Anticipated completion date: July 1, 2007.*

**We also recommend** that department management formally assign responsibility for timely resolving problems identified in all system error reports, consider making system modifications to enhance audit trail information, and ensure identified system reporting issues are resolved.

***Agency's Response:***

*The department agrees with this recommendation. A formal process for ensuring that system error reports are monitored, and that timely resolution occurs on any problems identified will be developed.*

*An aging report will also be developed and implemented, requiring the retention of check-based information that is in error.*

*Application modifications are currently in process that will enhance audit trail information and address system reporting issues identified.*

*Additionally, OIS will address and correct any other specific reporting issues that are identified. Anticipated completion date: December 31, 2007.*

### **Backup and Restoration Strategies Were Inadequate**

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

We noted that not all system files were adequately backed up. Specifically, only two of the six critical data files we tested were copied to tapes designated for off-site storage. In addition, roles and responsibilities for backup and recovery were not fully defined in department policies or procedures, or in the department's Service Level Agreement with the State Data Center.

Thus, we concluded it was unlikely the department could timely, or fully, restore system information exclusively from off-site tapes. In addition, efforts to restore the system subsequent to a disaster would likely be significantly hampered by the department's lack of a defined and tested recovery plan.

We concluded that these issues existed because the department had not clearly assigned responsibility for these important functions.

**We recommend** that department management develop, implement, and test complete system backup and recovery strategies. Items

needing specific and immediate attention include ensuring that all critical files are backed up and stored off-site, specific roles and responsibilities are defined and assigned, and backup and recovery efforts are formally coordinated with the State Data Center via a written service level agreement.

***Agency's Response:***

*The department agrees with this recommendation. The servers that support the Check Reconciliation System and Accounting Interface Applications reside at the State Data Center. DHS is a key participant in the Computer and Networking Infrastructure Consolidation (CNIC) Disaster Recovery (DR) Task Force, with the Office of Information Services (OIS) and the Information Security Office (ISO) as participants. The objective of this group is to coordinate SDC and agency resources in the development and implementation of DR strategies and practices. Through the activities of the CNIC DR Task Force and its workgroups, and in conjunction with DHS OIS DR activities a comprehensive DR plan will be developed to support the Check Reconciliation System and Accounting Interface Applications.*

*Anticipated completion date: The completion dates are dependent upon the project plans of the CNIC DR Task Force and its workgroups. On June 18, 2007, the CNIC DR Task Force presents its proposed course of action to the CNIC Governance Board for approval of its plan and commitment to resource allocation. Once approved, workgroup charters and project plans will be completed. Then the completion date can be projected.*

## Program Change Management Controls Should be Improved

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

Based on our review, we concluded that the department's change management controls did not always follow generally accepted change management practices. Specific control issues included the following:

- Department personnel did not perform independent technical reviews of program changes, including code-compare, prior to approving the changes.
- Prior to movement to production, approved code modifications were not appropriately safeguarded to prevent unauthorized changes. Rather, they were stored in a directory that was accessible to all members of the programming group.
- Members of the interface unit directly modified certain production data sets, contrary to best practices. All routine changes to production files should be made through the application or in a separate controlled environment.

As a result of the above control issues, department managers did not have reasonable assurance that all program modifications were appropriate. We concluded that these control issues existed because department management had not developed complete change management policies and procedures.

**We recommend** that department management develop more robust

program change management policies and procedures to:

- Require independent technical reviews of code modifications prior to approval and elevation to production, and consider using software code-compare utilities to further ensure only authorized changes are made.

### **Agency's Response:**

*The department agrees with this recommendation. The use of code compare software is being incorporated into the release management process. Anticipated completion date: March 31, 2008.*

- Further restrict logical access to code once it has been approved, and prior to moving it to production. This access should be granted only to individuals who, when authorized, will move the code into production.
- Ensure that modifications to production data sets are performed in a controlled environment outside of the production region.

### **Agency's Response:**

*The department agrees with this recommendation. A refined and more functional release management process, including policies and procedures, is being developed.*

*In addition, the existing formal change management process will be modified to include the agency's approach to application code and system changes, quality control and change management, and scheduling, testing and validation of changes prior to implementation.*

*Many of the changes or advancements require collaboration with the SDC. The CNIC DR Task Force is working to ensure adequate processes, procedures, roles and responsibilities for disaster recovery and daily operations are clearly understood and documented.*

*Anticipated completion date: March 31, 2008 is the anticipated completion date for the release management process changes and revised policies and procedures.*

*The completion date for the change management process is dependent upon the project plans of the CNIC DR Task Force and its workgroups. The CNIC DR Task Force is presenting its proposed course of action June 18, 2007 to the CNIC Governance Board for approval of its plan and commitment to resource allocation. Once approved, workgroup charters, project plans, and DHS' OIS activities will be completed. Then the completion date can be projected.*

## Logical Access Controls Should Be Improved

Executive management is responsible for establishing an overall approach to security and internal control to ensure protection of resources and to maintain integrity of computer systems. Logical access control is a vital part of an organization's overall security approach.

We concluded that the department's logical access controls did not adequately protect the system from unauthorized use, disclosure, modification, damage, or loss.

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

**We recommend** that department management implement the recommendations included in our confidential management letter.

**Agency's Response:**

*The department agrees with the recommendations in the confidential management letter. As requested, we will be providing a response by June 18, 2007.*

## Audit Scope and Methodology

We focused our review on the Combined Check Reconciliation System & Accounting Interface (system) as it existed after the first update project was implemented on September 1, 2006. Our review included application controls that governed interfaced input received from other check-producing applications and various general computer controls that affected system operations and maintenance.

During our audit, we interviewed department personnel assigned to the system. In addition, we examined technical documentation relating to the system and its architecture. We performed fieldwork between July 2006 and March 2007.

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

- verify that data stored in system tables conformed to documented system edits;
- validate the flow of data from input through processing and output; and
- validate system output files directed to the Statewide Financial Management Application (SFMA).

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

To test program change management controls, we evaluated the department's change management policies and procedures, reviewed logical access to file locations, and performed a limited review of documentation for changes.

We tested backup and restoration controls by reviewing backup procedures and logs of backups performed.

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

We conducted our audit according to generally accepted government auditing standards.



**Secretary of State  
Audits Division**

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

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

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

AUDIT STAFF: *Erika A. Ungern, CISA  
Robert M. Johnson, MBA  
Constance S. Bailey  
Nicole D. Real  
Gregory J. Klof*

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

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

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

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

*by phone at 503-986-2255*

*or by mail from:*

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