



Secretary of State Audit Report

Department of Human Services: Client Maintenance System Application Controls Review

Summary

PURPOSE

The purpose of our audit was to evaluate the effectiveness of key general and application computer controls for the Department of Human Services' (department) Client Maintenance (system) computer application. Our specific audit objectives were to determine whether the department had adequate controls governing data integrity, system security, program change management, and system backup and restoration.

RESULTS IN BRIEF

The system provided reasonable assurance that data input remained complete and accurate through data processing and output. However, the validity and completeness of data input was not always assured. As a result, during calendar year 2004 the department issued overpayments through the system to clients totaling approximately \$320,000.

The department's security framework did not adequately protect the system from unauthorized use, disclosure or modification, damage or loss. Because of the sensitive nature of security, we issued a separate report outlining specific details of our findings and recommendations to improve security in accordance with ORS 192.501 (23), which allows exemption of such information from public disclosure.

The department's program change management controls ensured that system modifications were tested and documented. However, those controls did not ensure program modifications were formally authorized or reviewed. In addition, access to program code was not sufficiently restricted to ensure it could not be altered after it was formally tested. If these weaknesses were exploited, the integrity and validity of the system could be compromised.

The department backed up system programs and files but had not developed disaster recovery and business continuity plans to restore the application in the event of a major disruption.

RECOMMENDATIONS

We recommend that the department:

- Seek appropriate recovery of the overpayments, correct identified system data errors, and implement either manual or automated controls to prevent future errors.
- Implement the recommendations included in our confidential security report.
- Improve program change management procedures.
- Work with the Department of Administrative Services to establish disaster recovery plans.

AGENCY'S RESPONSE

The Department of Human Services generally agrees with the recommendations.

Background

The Department of Human Services (department) implemented the Client Maintenance System (system) in the 1970s to monitor eligibility for benefits the department provides to qualifying Oregon residents.

The system provides information that the majority of the department's other computer systems use to manage benefit programs. In addition, the system issues certain payments to clients for Temporary Assistance to Needy Families (TANF), Oregon Supplemental Income Program (OSIP), and General Assistance. During calendar year 2004, these payments totaled over \$97 million.

The department's Office of Information Systems operates and maintains the system, which resides on the department's mainframe computer. In November 2003, Governor Kulongoski publicly announced an initiative to consolidate many of the state's data centers. The department is scheduled to be the first agency integrated into and serviced by the state's data center created under the Computing and Networking Infrastructure Consolidation (CNIC) initiative. The Department of Administrative Services tentatively estimates this move will occur during 2005.

Objectives and Purpose

The purpose of our audit was to evaluate the effectiveness of key general and application computer controls for the department's Client Maintenance (system) application.

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

- Data remain complete, accurate, and valid during input, processing, and output.

- Information assets are protected against unauthorized use, disclosure or modification, damage or loss.
- System program modifications follow approved system development processes and change management procedures.
- System files and data are appropriately backed up and could be timely restored in the event of a major disruption.

Audit Results

Application Controls Did Not Prevent or Detect Some Payment Errors

Effective application controls reduce the risk of unauthorized, inaccurate, or incomplete input, processing, output, and storage of transactions. These controls include either manual or automated routines that ensure only complete, accurate, and valid data are entered into a computer system; processing performs correct functions and results remain accurate; and data are properly maintained. Well-designed application controls include provisions for preventing erroneous data from being entered into the system as well as routines for detecting potential errors that may have occurred so they can be timely corrected.

The system used numerous automated application controls to ensure only valid client eligibility information was entered into the system. However, not all data was controlled through these automatic error-preventing or checking routines. In some instances, the department opted to rely on system users to manually ensure that they entered all the data the system needed to correctly calculate client benefits.

Based on our tests of data, we concluded that the system provided reasonable assurance that data

entered into the system remained complete and accurate through data processing and output. However, the validity and completeness of data input was not always assured when those processes were manually controlled.

During calendar year 2004, the department issued approximately \$320,000 in overpayments through the system to Oregon Supplemental Income Program (OSIP) clients. Those overpayments occurred because client data did not include a required income component used in calculating the benefit amount. Department staff indicated that the system did not have automated controls requiring users to provide the income information because in a few instances the information should be appropriately excluded. The overpayments represented approximately 3.7 percent of OSIP payments issued for the period and were funded entirely by the state's General Fund.

We concluded that the above overpayments could have been easily identified and prevented through automated error detection methods because they were unusual, repetitive and significantly larger than anticipated. The typical payment for OSIP clients was \$1.70 per month. However, many of the overpayments were for amounts in excess of \$500 per month.

We recommend that department staff correct identified system data errors and implement either manual or automated controls to prevent these overpayments from recurring. In addition, the department should seek appropriate recovery of the identified overpayments.

Agency's Response:

We partially agree.

In order for CMS to accurately perform the additional editing suggested, new data would need to be captured. CMS is thirty years old and not easily modifiable. The

master record has no room for additional items. This means that we have to use existing code structures to represent new information. In order for the system to perform any meaningful edit(s), the worker would be required to enter a code that would represent the situation in which the OSIP client's income could be excluded. Hence, we would still be relying on the worker to determine the values to enter. They would have to enter either the income or the reason for not recording the income. It does not appear changes would be cost effective or provide additional levels of control. We would still be relying on the worker to make the correct assessment.

We have begun the process to recover the identified overpayments. In April 2005, SPD central office staff requested a computer-generated list of probable cases with inappropriate cash payments sent to OSIP clients. Our Medicaid Program Analyst reviewed each case for correct coding and payment. Local office program managers were given the names of any client receiving a cash payment in error. Local offices were instructed to have the case coded correctly, send the client a reduction notice and calculate the overpayment. We will repeat this process each month after compute deadline so that Central Office staff can review cases within the first 30-days of any inappropriate payment.

System Data and Programs Were Not Appropriately Protected

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.

Based on our tests of security, we concluded that the department's security framework was not

adequate to protect the system from unauthorized use, disclosure or modification, damage or loss.

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

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

Agency's Response:

We will respond to those issues separately upon receipt of the final confidential report.

Program Change Management Procedures Were Insufficient

Effective change management procedures should ensure that program modifications are appropriately authorized, documented, thoroughly tested and approved by management before they are placed in production. Those procedures should also ensure that program modifications adhere to programming standards.

The department's change management processes ensured program changes were documented and tested. However, those procedures did not ensure:

- Changes were formally authorized and approved by management before they were performed.
- Independent reviews of program modifications were performed to ensure that only intended changes were made.
- Program code was sufficiently restricted to ensure it could not be altered after it was formally tested.

As a result, errors or unauthorized code could be introduced into the system without being detected. The ultimate risk associated with these weaknesses is that the integrity and validity of the system, its data, and those systems that rely on system information could be compromised.

We recommend department management develop and implement procedures to ensure that system changes are authorized, approved by management, and are independently reviewed. In addition, programmer access to modified code should be strictly limited after it is submitted for final review.

Agency's Response:

We agree. OIS has recently implemented a Change Advisory Board (CAB). All system changes to source code must be presented to the board for review prior to movement into production. Emergency code changes are reviewed at later CAB meetings.

Additionally, OIS recently filled a Quality Assurance Team Lead position that is part of the Application Architecture Group. This position will help insure that formal testing processes are applied consistently throughout the Department.

As can be seen by these recent initiatives, this is an issue that OIS recognizes as requiring attention and steps are being taken to improve our processes in this area.

Disaster Recovery and Business Continuity Plans Were Not Developed

Disaster recovery and business continuity plans are critical controls for safeguarding assets in the event of a disaster. Backup and offsite storage of critical system files are also necessary for recovering information systems should a major disruption of services occur.

Although the department backed up system programs and files, it had not developed disaster recovery and business continuity plans to restore the application or business operations in the event of a disaster.

The system is a cornerstone application to the department's public assistance and medical programs. Therefore, the inability or a significant delay in recovering this system may pose an unacceptable risk.

We recommend the department work with the Information Resources Management Division of the Department of Administrative Services to establish a disaster recovery solution that will be congruent with the consolidated data center initiative.

Agency's Response:

We agree. DHS will address the disaster recovery and business continuity plan (BCP) issues referenced in this audit through two current projects.

The first project is the DHS migration to the State Consolidated Data Center (SCDC). During this project, DHS will work with other State agencies to define service level agreements for a number of items to include in disaster recovery plans. All systems and data of similar sensitivity and value will be protected equally.

The second project is the DHS BCP that will initially address 126 mission-critical functions identified by DHS. This project supports the Statewide BCP effort being facilitated by DAS. DAS has procured tools and training to assist DHS in completing the BCP associated with the client maintenance system application. Once DHS training is complete (scheduled for July 2005), the Information Security Office will develop and implement a schedule for the 126 mission-critical functions.

Scope and Methodology

During our audit we interviewed various department personnel, examined system documentation, and analyzed electronic data.

The department's input controls primarily centered around automated edit and relational controls within the system. As a result, our review of input controls was similarly limited.

We reviewed automated edit and relational controls existing within the system as of August 1, 2004. Our tests of processing controls were performed against data processed on September 3, 2004, and September 7, 2004. We also obtained additional data from calendar year 2004 to review selected client payments.

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

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



**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 Weatherspoon, CPA, CISA, CISSP*

AUDIT STAFF: *Dale Bond, CPA, CISA, CFE
Chris Knutson
Jason Robinson, CPA
Ben McClelland*

DEPUTY STATE AUDITOR: *Charles A. Hibner, CPA*

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/audithp.htm>

by phone at 503-986-2255

or by mail from:

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