

Secretary of State AUDIT REPORT

Report No. 2003-12 • March 21, 2003

Oregon Employment Department: Review of Oregon Benefit Information System Controls



Bill Bradbury, Secretary of State
Cathy Pollino, Director, Audits Division

Summary

BACKGROUND AND PURPOSE

The Employment Department's Oregon Benefit Information System (OBIS) processes unemployment assistance claims for qualified unemployed workers. The purpose of our audit was to evaluate controls ensuring data integrity, system security, program change control, and business continuity.

RESULTS IN BRIEF

The system produced reliable data. Unemployment benefits were calculated correctly and key data remained valid within the system during processing and update; however, the department's efforts to secure the system were insufficient. Security areas needing improvement included controls over screen-level access, and safeguards to protect production files and data. Security policies and procedures were also incomplete. Significant opportunities for improvement also exist regarding controls governing system maintenance and business continuity.

RECOMMENDATIONS

We recommend that the department:

- Reevaluate and adjust its methods for providing screen-level access to OBIS.

- Further limit access to production files.
- Update its security policies.
- Improve formal methodologies governing system maintenance.
- Develop, implement, and test a more comprehensive business continuity plan.

AGENCY RESPONSE

Employment Department management generally agrees with the recommendations.

The Employment Department is pleased that the Audits Division provided the time and effort to evaluate the systems controls of our Oregon Benefits Information System (OBIS). As noted in the audit report, this is a mission critical system that provides important contributions to Oregonians and to the Oregon economy. Below are our responses to the draft audit report.

Background

The Oregon Employment Department (department) uses the Oregon Benefit Information System (OBIS) to process unemployment benefit claims. In calendar year 2001, the department paid over \$688 million in unemployment benefits. Although the department has staff dedicated to operate and maintain OBIS, the computer application resides on the Department of Human Resources' mainframe computer.

Objectives, Scope and Methodology

The objective of the audit was to determine whether application controls of the Oregon Benefit

Information System were in place and functioning to ensure that:

- Unemployment claims remained complete, accurate and valid during system input, processing, update and storage.
- Program and data files were safeguarded and system use was restricted based on individuals' demonstrated need to add, modify or delete information.
- Modifications to the application were properly controlled.
- The business functions supported by the application could be timely resumed in the event of a disaster or other interruption of regular service.

To meet these objectives, we reviewed system documentation, interviewed department personnel,

recalculated benefit payments, and examined source documents. We based our conclusions regarding the completeness and reliability of the data on direct tests of the data.

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

Audit Results

OBIS Data Has Integrity

The Employment Department's Oregon Benefit Information System (OBIS) produced reliable data. Specifically, unemployment benefits were calculated correctly, key data contained in the various files within the system remained consistent, and payments were consistent with system calculations.

Agency's Response:

Agree: The system is reliable and provides correct calculations, as noted in the report. This is the most significant observation of the audit team, since it validates the overall operational quality of the system itself. The department is pleased that the audit team has independently verified that the core components of the Benefits System perform as designed.

OBIS Security Should Be Improved

The department's efforts to safeguard the system were insufficient. Specific areas needing improvement included the following:

- Security software designed to restrict individual users' access to the various program screens and functions was not used as intended.
- Access to production data files and programs was not sufficiently restricted.
- Security policies were incomplete.

Screen-Level Access Code Was Not Functioning as Intended

Mechanisms should be in place to restrict users' access to system data and functions. Access privileges given to individuals should be based on users' unique need to view, change or delete information or utilize system resources. One common method for facilitating this security function is to implement security software that uses identification, authentication and authorization routines that link users and resources with access rules.

Although the department developed security software to control screen-level access to the system, that software was not implemented as originally designed for most users. Department

programmers bypassed the security application by writing code into individual OBIS programs; in addition, they did not sufficiently document their programming changes affecting the security system.

As a result, the department could not readily ascertain what access privileges individuals and user groups actually had, or were intended to have. In addition, changes to access levels for bypassed users could be accomplished only by changing program code. This scenario significantly increased the risk that an individual or group had, or would be given, inappropriate access to system data or resources.

We recommend that the department reevaluate and adjust its methods for providing screen-level access to OBIS. The department's solution should ensure that users are given access that is unique to their needs. It should also allow for routine security maintenance without modifying OBIS programming.

Agency's Response:

Agree in principle: The Employment Department Security System (EDSS) was created prior to the implementation of Remote Access Control Function (RACF) on the DHS mainframe. Many of the newer components of the OBIS system utilize RACF security; however, the department will evaluate the impact of upgrading all the OBIS sub-systems to exclusive RACF security. Previous evaluations have indicated that this would be a significant effort that would need to be balanced against on-going production requirements.

Access to Production Files Was Not Appropriately Restricted

To ensure that unauthorized or unintended changes to program code and data do not occur, access to production files and data should be

strictly limited and closely monitored. Best practices for system development, maintenance and operation indicate that programmers should not have routine access to the production region. If access to production files is given to programmers during emergencies, their actions should be closely monitored and validated. Generally, access to production files should be given only to an independent group responsible for moving programs from the test environment into production, and to assigned database administrators.

The department assigned various staff including application programmers broad access to the production environment contrary to best security practices. We found that 52 user IDs had the ability to change production object code and move code into the production region. However, only a small group should have been given those powerful access privileges. Furthermore, we noted that 71 additional user IDs had unjustified read access to production object files.

During our review, we also noted that access to program test environments, production data, and program source code was not sufficiently restricted.

We recommend that the department further limit logical access to OBIS test and production program and data files according to best security practices. Programmers' access to the production region should be limited to closely monitored emergencies.

Agency's Response:

Agree in principle: Having an independent group responsible for moving programs into production files is an ideal practice. However, it may not be the best solution for our environment, including the amount of resources available. We do have controls in place to restrict the movement of object code into production libraries and

modification of production procedures and job control language. The department will review internal procedures to ensure that the movement of programs into production is appropriately restricted.

The report noted that 71 additional user IDs had “unjustified” read access to files. We believe that the additional programmers with read-only access is justified by their job requirements and information needs. However, the department will review those access privileges to ensure that they reflect correct business needs.

The Department’s Security Policies Were Incomplete

For security to be successfully implemented and maintained, management must clearly establish and communicate to all appropriate parties the framework and intent of security. A security policy should establish the organization’s overall approach to security and internal control to ensure protection of resources and maintain integrity of computer systems.

The department’s overall security framework was incomplete. Key components not adequately addressed included the following:

- Processes for periodically confirming users’ access rights.
- Procedures to ensure that all data are classified in terms of sensitivity and secured according to data access rules.
- Measures to promote and maintain security awareness among all employees.

We recommend that department management update its security framework policies to include the above components.

Agency’s Response:

Agree in Principle: During the audit field work, the current security policy was in draft form. It was

completed and adopted in November 2002. Since the audit finding references a security policy that has since been updated, we acknowledge the comment. The new policy includes all key components recommended by DAS and by ISACA (Information Systems Audit and Control Association.).

The department has a three-step process for assuring that access rights are terminated when needed. Subsequent reviews have shown this process to be sufficient to minimize the risk of unauthorized continued access. This contributes to the key component of Ensuring Systems Security.

Data classification is a highly sophisticated, detailed, and time intensive process to identify, classify, and secure each individual piece of data in a system. The department instead classifies and secures each database or system of data based on the most sensitive information contained in it. This provides sufficient information to protect our data. This also contributes to the key component of Ensuring Systems Security.

The department has always communicated and maintained security awareness among all employees. For example, each employee must sign a statement that they have read and understand our confidentiality policy before they are allowed to start work. Security and confidentiality are discussed in our New Employee Orientation. Managers discuss security issues during staff meetings. These measures serve to create and maintain a culture of protecting confidential information. This contributes to the key component of Communicating Management Aims and Direction.

System Maintenance Procedures Need Improvement

A system maintenance methodology should exist to manage changes made to computer systems. This methodology should include appropriate procedures for requesting, performing, testing, documenting and obtaining management approval before a change is made to production code. In addition, circumstances should be defined as to when system maintenance can be performed outside of normal procedures. These emergency circumstances should have their own procedures to control and document changes.

The department’s system maintenance methodology did not provide a reasonable level of assurance that only approved and tested changes were made to the OBIS.

The department’s procedures did not provide detailed guidance for the creation and use of testing plans, review of test results, performance of user testing, and the creation and retention of testing documentation. In addition, formal procedures did not exist governing emergency changes. Finally, formal procedures were not adopted for projects originating within the information technology unit.

When procedures did exist, department management did not always follow them. For example, the information technology unit’s OBIS Manager gave approval for both the user and the IT section before moving changed OBIS program code into production. The department’s procedures called for separate user approval of changes to the OBIS.

We also found that department management did not sufficiently monitor staff during system maintenance and did not enforce proper segregation of duties. Management generally did not

review the changes made by programmers before the changed code was used in production. Management also did not use automated tools, such as code comparisons and version tracking, to monitor the changes made to the system. Furthermore, management assigned incompatible responsibilities to some programming staff by assigning them to change program code, test the changes, and move the modified program code into production.

Management relied upon the integrity of their employees to access only the code or data they needed to do their jobs, to not make any unauthorized or unintentional system changes and to complete system maintenance as expected.

Without an adequate methodology governing system maintenance, the agency is at greater risk for disruptions, unauthorized alterations, or errors being introduced into the system and remaining undetected.

We recommend that department management improve its system maintenance methodology by developing and implementing:

- Policies and procedures for testing program modifications that require creation of testing plans, performance of tests, and creation and retention of testing documentation.
- Policies and procedures governing emergency program modifications and programming changes initiated within the information technology unit.
- Policies and procedures to more closely monitor program modifications to ensure code comparisons and improve version tracking. The department should consider using automated tools to accomplish these tasks.

We also recommend that the department reassign the task of moving program code into production to someone independent

from the application programming group.

Agency's Response:

Agree: Some of the policies and procedures recommended are in place, but are not uniform. The department is working to create and implement these policies. The department has contracted with a vendor to review the use of automated tools to improve testing processes. An RFI is expected to be released in the near future.

Business Continuation Planning/Disaster Recovery Planning was Incomplete

Management is responsible for ensuring that the agency can continue or resume operations following a disaster or other interruption of services. Department management is therefore responsible for implementing a proper strategy for the backup and restoration of information assets that considers the agency's business requirements.

A sound strategy would include the development, documentation, implementation, periodic testing, and maintenance of a detailed recovery plan. Additional procedures should ensure that backup copies of programs and data are created and stored offsite in accordance with the plan. There should also be a requirement that the plan be reviewed regularly to ensure that the plan continues to satisfy the agency's requirements. The plans should assume that some or all of the agency's key people would not be available to assist in the recovery process.

The department's planning for disaster recovery and business continuity did not adequately provide for the continuation of unemployment benefit payments in the event of a disaster or other major interruption of service. The department did not have an effective plan for the recovery of the OBIS, and was dependent on another state

agency that also lacked an appropriate recovery plan.

The department had a recovery plan designed to have key personnel meet, assess needs, and determine an appropriate strategy to restore system functionality once an incident has occurred. However, industry standards suggest that recovery plans also include specific procedures for recovering from the various incident scenarios that may face the organization. The department's plan was incomplete because it did not include these specific procedures to address various recovery alternatives.

The department maintained program and data files at an offsite storage facility. The files, however, did not include everything needed for full recovery following a significant interruption in service. During our audit, management identified a number of useful backup files that were not stored offsite. Subsequently, back-up copies of these files were moved offsite. In addition, copies of system documentation and other materials to be used in recovery were not stored at the offsite facility.

The system resides on the Department of Human Services' (DHS) mainframe. Therefore, the department is dependent on DHS's ability to restore the mainframe in the event of a major disruption. Our audit of DHS general controls (Report No. 2001-55) found that the DHS data center's disaster recovery planning did not provide assurance that critical services could be timely continued in the event of a disaster.

The Service Level Agreement between the department and DHS did not adequately address the services needed by the department in the event of a disaster. The agreement did not specify how quickly restoration of the system was to occur, or the order in which DHS and department application systems would be restored.

The department had not fully tested its plan, including recovery of systems and applications offsite. Although department procedures required annual testing of the disaster recovery plan, testing had not gone beyond tabletop exercises conducted in preparation for the year 2000 date change. These conditions were not an industry best practice.

Without adequate business continuity planning, the department is at increased risk of not being able to ensure the timely continuation of unemployment benefit payments in the event of a disaster or other major interruption of service.

We recommend that department management:

- Clarify its strategy for ensuring the continuation of critical business functions in the event of a disaster or other interruption of services.
- Adopt a policy to ensure the development, implementation and maintenance of business continuation plans that would include disaster recovery planning for the associated computer applications.
- Improve the Service Level Agreement with DHS, by including sufficient detailed

requirements to ensure that DHS would provide the level of services needed for the department to recover its mainframe systems in accordance with the time lines in the department's plans. The agreement should also clarify the priority accorded to the various department and DHS applications during the recovery process.

- Conduct periodic testing of the business continuation plans.
- Adopt formal backup procedures, including the identification of critical files for back up and periodic testing to ensure that the back ups are created and stored in accordance with the procedures.
- Identify and store those items needed for recovery and continued operations at an off-site facility.

Agency's Response:

Agree in principle: While the department has an excellent record of uninterrupted service from its Benefits System, disaster recovery planning is an area that will always benefit from improved planning and rehearsals. The methods and procedures that we use for backup and recovery of data files and

libraries are, in fact, tested on a regular basis. VSAM files are deleted, redefined, and reloaded frequently, as part of our nightly batch processing. DMS is used frequently to restore library members and occasionally entire libraries. We currently run nightly batch jobs that create offsite backup tapes of our critical OBIS VSAM files. However, the department will examine opportunities to improve its disaster recovery readiness. For example, the department will benefit from the current disaster recovery planning that is jointly being pursued by the Departments of Administrative Services, Human Services and Transportation. The department will join in the efforts of these agencies to work toward a common data center hot site for emergency operations. The Service Level Agreement with DHS will be updated to include appropriate recovery processes. The department will also refine its current disaster recovery and business continuation planning to address specific scenarios, and will plan for periodic testing of these plans. Policies and procedures will be updated to address backup and recovery expectations.

This report, which is a public record, is intended to promote the best possible management of public resources. Copies may be obtained by mail at Oregon Audits Division, Public Service Building, Salem, Oregon 97310, by phone at 503-986-2255 and 800-336-8218 (hotline), or internet at Audits.Hotline@state.or.us and <http://www.sos.state.or.us/audits/audithp.htm>.

AUDIT ADMINISTRATOR: *Neal E Weatherspoon, CPA, CISA*

AUDIT STAFF: *Mark A Winter CPA, CISA • Jamie E Breyman • Wendy M Kam • Virginia L Teller*

DEPUTY DIRECTOR: *Charles A Hibner, CPA*

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

Auditing to Protect the Public Interest and Improve Oregon Government
