

AUDIT REPORT

Department of Human Services: Evaluation of General Computer Controls



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

Summary

PURPOSE

The purpose of this audit was to evaluate general computer controls at the Department of Human Services' (department) data center. General controls protect the environment in which software applications process data. These controls relate to security, disaster recovery and contingency planning, and management of day-to-day operations. Our audit work included a review of the department's efforts to implement prior audit recommendations.

RESULTS IN BRIEF

The department has not provided adequate physical security for its data center nor has it sufficiently restricted data center employees' access to systems and data. In addition, the department has not developed adequate disaster recovery and contingency plans to ensure timely resumption of data center operations. Furthermore, the department needs to strengthen several operational controls.

The department has not implemented a significant number of prior audit recommendations. We have integrated these issues within the context of the findings in this report.

RECOMMENDATIONS

We recommend that department management:

- Further restrict physical access to the data center, and ensure that data center employees have access to only the systems and data they need to perform their duties. In addition, management should ensure that their ongoing efforts to develop an overall security framework policy addresses data center needs.
- Fully develop disaster recovery and contingency plans.
- Strengthen operational controls at the data center and provide regular reviews of controls.

AGENCY RESPONSE

The Department of Human Services generally agrees with the recommendations.

Introduction

Background

The Department of Human Services (department) is Oregon's health and social services agency. Its Office of Information Services operates a data center that hosts the department's significant payment systems and other software applications. The data center also provides computing services for the Employment Department.

On August 28, 2001, we released an audit report on the adequacy of the department's security controls for computer applications. This report, No. 2001-37, *Oregon Department of Human Services: Security Controls for Computer Applications*, included recommendations for developing a more comprehensive solution for securing the department's

information systems and data. In response, department management indicated that they would establish a security task group to develop a long-term security framework to better meet the department's security needs.

During our review of data center security, we considered the results of the above mentioned audit report, as well as the agency's on-going efforts to provide security for its systems and data.

General Computer Controls

General controls protect the environment in which software applications process. These controls include processes and procedures to ensure security of data and systems, continuous service in the event of a disaster, and management of day-to-day operations. Department

management is responsible for ensuring that the data center has adequate general controls.

Audit Results

Data Center Security Should Be Improved

The department should have a comprehensive policy establishing how it safeguards information systems and data. This policy should include procedures and methodologies for limiting physical access to the data center. In addition, it should include logical access controls to ensure that only authorized users have access to systems, data and programs.

Since the data center houses critical systems, physical access to the data center should be restricted to only authorized individuals who

work there. Others needing temporary access should be appropriately escorted and supervised while in the data center.

Data center workers need logical access to certain system resources in order to perform their assigned duties. Data Systems should be controlled by security software that allows individuals access to certain information while restricting their access to other information. Access to resources should be strictly monitored and limited based on the individuals' demonstrated need.

Breaches or weakness in data center physical or logical security could result in system failure, unintended disclosure of confidential data or loss of data integrity. Such failures, which could be accidental or deliberate, may compromise the department's ability to provide critical services to clients.

The department has not provided adequate physical or logical access controls for its data center. This resulted, in part, from the department's lack of an overall security framework policy. However, many security weaknesses occurred because existing security systems and procedures were not effectively managed. Significant security issues included the following:

Physical Security Weaknesses

- Contracted service providers had unrestricted, unsupervised access to the data center and its resources.
- More than 70 Department of Administrative Services custodians and maintenance employees also had unrestricted and unsupervised access to the data center.
- The department did not revoke physical access privileges for many individuals who no longer needed to enter the data center.

- Employees could not account for many data center keys or electronic key-cards.

Logical Access Control Weaknesses

- Department management gave data center employees access to programs and data that they did not need to perform their assigned duties.
- Management of user IDs and passwords was inadequate to ensure effective utilization of the security software.
- The department did not always perform criminal background checks on individuals accessing the data center and systems.
- Security tasks were not appropriately separated to ensure the integrity of the security system.

We recommend that the department take immediate steps to ensure that data center security risks are reduced to a more appropriate level. Specifically, the department should restrict all access to the data center and its resources to those with a demonstrated need for those resources. Furthermore, it should ensure that no individual is provided unsupervised access that could potentially allow him or her to compromise critical processes or information technology resources. Furthermore, as the department develops a security framework policy, it should ensure that physical and logical access at the data center are appropriately considered in its overall approach.

Agency's Response: We agree.

This will be fully addressed in the security framework being planned by the Department, especially logical and data access. Specifically, Computing Resource Management (CRM) is working on implementing additional physical security measures including a double-barrier entry system as defined by the Internal Revenue Service. In addition, a procedure is

being developed to regularly verify the need of all individuals who have access to the computer center and its resources. We will:

- *Use state personnel data to verify employment for all state staff against the list of employees needing access in the security system,*
- *Use internal DHS forms which are already filled out for staff leaving DHS to remove staff from the security system,*
- *Verify on a regular basis the state employees who need access to the data center and its resources; we are working with Department of Administrative Services (DAS) Facilities staff to verify and clean up the list of maintenance and custodial staff who are currently in the security system,*
- *Verify on a regular basis those vendor employees who need access, and*
- *Revisit and strengthen the visitor badge procedure, modeling it as much as possible after the procedure used in the Human Services Building.*

Disaster Recovery Plans are Incomplete

Disaster recovery and contingency planning is necessary to ensure that services will be provided in the event of a disruption. These plans should include procedures to regularly backup information system programs and data and store them in a secure off-site location to ensure redundancy. They should also include detailed procedures for recovering from various disaster scenarios. Furthermore, the plans should provide alternate processing facilities for use until the data center resumes operations.

Without adequate disaster recovery and contingency planning, the department may not be able to timely restore critical information

systems that provide vital business functions.

The department has not developed adequate disaster recovery and contingency plans to ensure timely resumption of data center operations. Significant issues included the following:

- Although data center staff has documented various procedures for recovering limited mainframe capability at an alternate processing facility, the procedures were incomplete. For example, they did not consider recovery of mission critical applications and network communications.
- In addition, the department relied on a month-to-month agreement for its alternate processing facility. Its previous contract expired in April 2000.
- The department's offsite storage facility was inadequate because it was too close to the data center, and thus subject to the same vulnerabilities and threats.

We recommend that department management fully develop disaster recovery and contingency plans, obtain a formal contract for ensuring use of an alternate processing facility, and secure a more appropriate offsite storage facility.

Agency's Response: We agree.

DAS is establishing a disaster recovery contract for DAS General Government Data Center, the ODOT data center, the Revenue data center, and the DHS data center. This effort has been assigned a DAS project manager and will analyze business impact. The award for a new disaster recovery site is planned for the March-April 2002 timeframe.

CRM is working with DAS to acquire a new offsite storage facility for the DAS, ODOT, and DHS computer centers. This facility should be selected and in place sometime in the first quarter of 2002.

Operational Controls Should Be Strengthened

The department is responsible for providing adequate services to data users. These services should include accuracy, completeness, timeliness, and proper distribution of output relating to application processing. It should also provide for efficient operations and properly controlled changes to system software. To ensure that these important functions are carried out, the department should regularly monitor the effectiveness of data center operations and controls.

Weak operational controls could result in unintended disclosure or loss of confidential or sensitive data, system failure, loss of data integrity, and misuse of resources. Such weaknesses may also compromise the department's ability to provide critical services to clients. Significant issues relating to data center operations include the following:

- The data center did not have written procedures to ensure that system software changes are made in a systematic and controlled manner.
- Employees did not always follow established procedures designed to control full or partial system shut downs.
- Management did not have procedures to protect its data media library contents by controlling the physical movement, storage, and accountability of data cartridges. As a result, several cartridges were missing from the library and others were found in a public hallway outside the data center.
- The data center did not have adequate procedures to ensure that data cartridges destined for disposition were erased.
- Data center management did not adequately monitor software-licensing agreements.

- Management did not adequately safeguard checks or check stock by performing inventories of check stock, maintaining accurate and complete control logs, securing checks printed on the weekends, and providing adequate custodial transfer of printed checks.
- The department has not provided regular, independent reviews of data center controls.

We recommend that the department strengthen operational controls at the data center by developing and implementing procedures to control system software changes, govern media library functions including disposal or disposition of data cartridges, monitor software agreements, and safeguard checks. In addition, the department should provide regular reviews of data center controls to ensure that controls are working as intended.

Agency's Response: We agree.

All the operational controls mentioned are being implemented except for the independent reviews, which will be set up once the other controls are fully functional. Specifically:

- *Procedures have been developed regarding system software changes. These procedures will be revisited, updated as needed and followed.*
- *The procedure for full or partial system shutdown will be reviewed to make sure it is up-to-date with the understanding that there will always be situations when the system will have to be shutdown and brought back up without following this procedure.*
- *We now have procedures to prevent tapes from being stored in unsecured areas and to prevent misplacing tapes.*
- *There are procedures and processes in place to erase data cartridges destined for disposal or other disposition.*

- *Software license agreements are being renegotiated, updated, filed, and monitored through an ongoing process vendor by vendor.*

Follow Up of Prior Audit Recommendations

During our audit, we reviewed the department's efforts to implement prior audit recommendations. Our prior audit report No. 98-49, *Department of Human Resources Computer Center General Controls Review*, included 22 audit recommendations, of which eight were either fully resolved or were no longer applicable. The remaining 14 unresolved or partially resolved issues are integrated within the context of the audit findings in this report.

Objectives, Scope and Methodology

Our audit included a review of selected general computer controls at the Department of Human Services data center. We performed our fieldwork between April and July 2001.

The objectives of our audit were to evaluate the adequacy of controls governing the following:

- data center security,
- logical access to electronic systems,
- disaster recovery and contingency planning, and
- day-to-day operations of the data center.

We limited our review of the department's logical access controls to those affecting data center employees.

Our audit work included inquiries of department personnel, examination of documents related to controls and procedures, and observation of information systems control processes and operations.

We evaluated compliance with applicable laws, rules, and regulations pertaining to internal controls and the operation of the data center. We also reviewed the status of related recommendations contained in our previous audit of the data center, issued in 1998.

During our audit, we used the Information Systems Audit and Control Foundation's (ISACF) publication "Control Objectives for Information and Related Technology" (COBIT) to identify generally accepted and applicable internal control objectives and practices for information systems. ISACF is a worldwide organization dedicated to researching, developing, and publicizing generally accepted information technology control objectives and audit guidelines.

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

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/auditthp.htm>

AUDIT ADMINISTRATOR: *Neal Weatherspoon, Audit Administrator, CPA, CISA*

AUDIT STAFF: *Dale Bond, CPA, CFE • Diana Barkelew, CPA • Michelle Rock, CPA*

DIRECTOR: *Cathy Pollino, CGFM*

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

Auditing to Protect the Public Interest and Improve Oregon Government