

Secretary of State AUDIT REPORT

Report No. 2001-51 • November 15, 2001

Oregon Department of Transportation: Data Center General Controls Review



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

Summary

PURPOSE

The purpose of this audit was to evaluate the adequacy of general controls in place at the Oregon Department of Transportation data center. General controls protect the environment in which software applications process data. These controls relate to backup and recovery, physical and logical security, systems development activities, facility management, the organizational structure, and independent audit. We included a follow up of prior audit findings.

RESULTS IN BRIEF

The Oregon Department of Transportation (department) data center's general controls could be improved to further protect its equipment and people. Many of the weaknesses noted were addressed in prior audit reports.

RECOMMENDATIONS

We recommend that management:

- Make disaster recovery and contingency planning a priority to ensure that services can be restored in the event of a disruption.

- Fully develop, implement and enforce policies and procedures to limit physical and logical access to its equipment and data.
- Fully develop, document and implement formal systems development methodologies addressing systems software and hardware.
- Fully develop and implement procedures to protect its systems and people from environmental hazards.
- Follow its policy regarding annual performance appraisals and training plans.
- Provide periodic internal audit reviews of the data center.

AGENCY RESPONSE

The Oregon Department of Transportation generally agrees with the recommendations.

Background

The Oregon Department of Transportation's (department) mission is to provide a safe, efficient transportation system that supports economic opportunity and livable communities for Oregonians. The department relies heavily on various information systems to carry out its mission.

The department's Information Systems (IS) section consists of five units, one of which is the Technology Management (TM) unit. The TM unit operates the department's data center and provides support related to system security, network and mainframe operations and telecommunications.

The department's IS section must seek reimbursement for the cost of providing services to other state

agencies, as well as other sections within the department.

On February 26, 1999, the governor signed Executive Order EO 99-05 directing the operational alignment of the Department of Administrative Services data center with the department's data center. We have issued Management Letter No. 107-2001-10-05 to the Department of Administrative Services addressing the operational alignment.

Information System Controls

Information system controls are typically classified as general controls or application controls. General controls protect the environment in which software applications process data. Application controls relate to

specific processing requirements of individual software applications. General controls coupled with application controls provide more assurance that transactions processed through the system are authorized, reliable and complete.

General controls focus on procedures pertaining to disaster recovery and contingency planning, facility management, physical and logical access, development methodologies related to system software and hardware, the organizational environment, and independent audit. If general controls are not working as intended, an agency may risk exposure to unauthorized access, damage to its systems and data, loss due to environmental hazards, and inability to fully recover in the event of a disaster.

Audit Results

Ensuring Continuous Service

Disaster recovery and contingency planning are necessary to ensure that services can be restored in the event of a disruption. These plans should provide detailed instruction for recovery from various disaster scenarios and be updated and tested on a regular basis.

Although the department has developed some disaster recovery and contingency plans, the department has not made recovery of its operations a priority. The plans are out of date, tests were last performed in 1996, and recovery team members are not aware of their responsibilities. Furthermore, elements of these plans are incomplete or missing important information, including the following:

- Various disaster response scenarios from minor to total loss of capability and responses to each, in sufficient detail for step-by-step execution.
- Detailed lists of equipment and supplies necessary to recover operations.
- Written agreements to ensure that vendors will provide expected services and that alternate recovery locations will be available and feasible in the event of a disaster.

In addition, the department's offsite storage facility is not located far enough away from the data center so as not to be affected by the same disaster. Furthermore, the department has not identified all the items needing to be stored at the offsite facility and those items that have been identified as needing to be stored offsite were not found.

In the event of a disaster, the department may be unable to fully recover all its business operations.

We recommend that management make recovery of its operations a priority by:

- Fully developing, implementing, and maintaining disaster recovery and contingency plans.
- Conducting periodic testing of those plans and training recovery team members.
- Relocating its offsite storage facility to a location that would be less affected by the same disaster and storing those items needed for recovery at the offsite facility.

Physical Access Controls

Management is responsible for providing controls that limit physical access to its computer system. Those controls should ensure that access is restricted to authorized individuals and potential violations are reported and resolved.

The department uses computer-controlled keycard locks to control access to its data center. In order for an employee or vendor to obtain a permanent keycard, a manager must complete an authorization form and the individual must pass a criminal history background check. The data center also issues temporary keycards to individuals needing access for a short period of time. Visitors to the data center are required to sign in and out on a log and be escorted by an authorized employee.

Although these controls help to limit access, they could be improved. Weaknesses identified include the following:

- Some employees and vendors continued to have access after their termination dates. One employee's keycard was still active one year after terminating employment.
- Not all individuals who have access to the data center have an apparent need for such access, including DAS Facilities office

employees, the landscape supervisor, and the Oregon State Police Office of Emergency Management. Of those having access, only 34 percent actually obtained access to the data center during the period reviewed.

- Documentation does not support that all employees and vendors with access to the data center have passed a criminal history background check.
- Visitor logs were incomplete and not reviewed.
- Procedures for issuing temporary keycards do not require formal manager approval and criminal history background checks.

As a result, management is less able to protect its data and systems from unauthorized use. These weaknesses exist because management's policies and procedures are not adequate to ensure that only appropriate individuals have access to the data center. Specifically, management's procedures do not include monitoring access or conducting a periodic review and confirmation of those individuals having access. In addition, other agency management can authorize and issue keycards to the data center without the department's authorization and knowledge. Finally, management does not always follow its own policy for visitors to the data center and is inconsistent in its policy for conducting criminal history background checks.

We recommend that management:

- Further develop, implement and consistently enforce policies and procedures to limit access to its computer systems. Those procedures should include periodic review and confirmation of access privileges, formal authorization from the data center management to obtain access regardless of the origination, and monitoring access.

- Ensure that its existing procedures for conducting criminal history background checks and completing visitor logs are followed and consistently applied.
- Immediately revoke all keycard access for those individuals who do not have a demonstrated need for such access and for those the department did not authorize.

We also have made recommendations to the Department of Administrative Services Facilities Division in Management Letter No. 107-2001-10-05 regarding physical security of the ODOT data center. Specifically, the Facilities Division's current practices of awarding keycard access have weakened security within the data center. We recommend that the Facilities Division:

- Determine which of its employees need routine access to the ODOT data center and submit requests to the data center's management.
- Establish keycard access to the ODOT data center only upon formal approval by the data center management.

Logical Access Controls

Management is responsible for implementing controls to safeguard information against unauthorized use, disclosure or modification, damage or loss by restricting access to authorized users.

The department relies on various manual and automated controls to limit access to its systems. For example, the system is set to force periodic password changes. In addition, the department's policy requires requests for access to be approved by the employee's manager or other delegated designee, and for all users to be given a unique ID. The department's Computer Security Unit processes all access requests and relies on an automated system to track requests and the actions taken.

During our review, we identified the following areas in need of improvement:

- Some system parameters are not set in accordance with the department's policy.
- One user ID allows access to all system information, is shared among technical support employees, and has conflicting access privileges.
- Authorization of access is not always documented. In addition, the Computer Security Unit does not have a complete list of managers or other designees authorized to approve access.
- Not all user accounts were deactivated in a timely manner. Two employee's accounts continued to allow access three months after the employee's termination date.
- The department does not periodically evaluate its employees' access privileges to ensure that they remain appropriate for current work assignments.
- The department has not developed a data classification scheme that would allow those responsible for authorizing access to have the knowledge necessary to limit user access to only those resources needed.
- The department has not developed incident handling and formal escalation procedures to be followed in the event of a security incident.
- Users are not prohibited from sharing their passwords with technical support staff.
- Technical support employees have unrestricted access to production programs and data and may assist in application program development and support. In addition, management does not monitor the technical support employee's activities in production.

As a result, the department is less able to secure its systems and detect unauthorized attempts to gain access to its systems and data. This situation exists because management has not fully developed adequate security policies and procedures and does not ensure its existing policy and procedures are followed.

We recommend that management:

- Enforce its existing policy and procedures by setting system parameters in accordance with policy, ensuring all users have a unique ID, and documenting all requests for access.
- Modify its existing policy to require access to be revoked no later than the end of the employee's last workday and prohibit employees from sharing their passwords.
- Limit technical support employees access to the production environment and data, and monitor those activities.
- Develop and implement additional procedures to require periodic reevaluation of access privileges, create and maintain a data classification scheme, and establish incident handling and escalation procedures.

Acquire and Maintain Technology Infrastructure

The generally recognized standard for managing the maintenance of computer-based systems and the purchase of system software and hardware is to adopt comprehensive System Development Life Cycle (SDLC) methodologies. SDLC methodologies should include a series of steps or phases that have defined goals and target completion dates. The actual phases for each project may vary and system maintenance efforts may not require the same level of detail or phases as new applications.

Although the Technology Management (TM) unit has some

policy and procedures in place when making changes to its system software and hardware, the following weaknesses were identified:

- Review of selected purchases made shows that TM may not complete all necessary steps or phases. For example, TM could not demonstrate to what extent equipment had been tested before purchasing, user approval, implementation and post implementation reviews.
- Procedures for controlling changes to the system are informal and do not include all of the necessary steps to adequately control changes made. For example, system documentation including the operations manual is not updated or maintained and a quality assurance review is not conducted.
- The policy outlining responsibilities and deliverables related to software upgrades is not followed and responsible parties stated that they were not aware such a policy existed.
- Equipment is sent to surplus for resale without ensuring all data had been properly erased prior to disposal.
- Problem management procedures do not exist.

As a result, the department is at risk that disruptions, unauthorized alterations, or errors could be introduced into the system and possibly go undetected.

This situation exists because management has not fully developed adequate SDLC methodologies, or defined deliverables regarding system software and hardware. In addition, management does not ensure that its existing policy and procedures are followed.

We recommend that management:

- Fully develop, document and implement formal SDLC

methodologies addressing system software and hardware. Those methodologies should include missing steps and deliverables as identified above.

- Enforce its existing policy when making upgrades.
- Ensure that all data is removed from equipment and other media before sending to surplus.

Managing Facilities

Management should ensure that sufficient measures are in place to protect systems and people from environmental hazards such as fire, power fluctuations, and excessive heat and humidity.

The data center relies on various mechanisms, such as sensors and alarms, to ensure the safety of both equipment and people. In addition, management has delegated monitoring some of those mechanisms to the Department of Administrative Services Facilities Division.

Although mechanisms are in place, the following weaknesses exist:

- Data center employees have not received periodic training on how to use fire extinguisher equipment.
- Documented procedures do not adequately describe expected response scenarios for various environmental emergencies.
- Procedures are not in place to ensure that all environmental monitors are maintained and working according to specifications and inspections are not documented.

In the event of an environmental emergency, the data center may be less prepared or delayed in its response and incur loss to its equipment, data and/or people. These conditions exist because management has not established adequate procedures to address all emergency situations.

We recommend that management fully develop and implement procedures to protect its systems and people including:

- Periodic training to data center employees on the proper use of all emergency equipment.
- Ensuring environmental monitors are maintained and working as well as documenting inspections.
- Expected response scenarios for various environmental emergencies.

Organization and Relationships

In order to maintain an appropriate operating environment for its computer systems, management is responsible for ensuring that all personnel are adequately trained and understand its roles and responsibilities in relation to information systems.

Department policy requires managers to conduct performance appraisals and develop a training plan for each employee on an annual basis. In addition, new employees are to receive training in relation to their assigned duties and responsibilities.

Review of selected employee's personnel files and interviews identified that managers did not always follow the department's policy to complete performance appraisals and training plans. Of the nine employees reviewed, six employees' last performance appraisal was dated between 1991 and 1997 and three employees did not have a current and formal training plan on file. In addition, the data center's new employee training materials are outdated.

As a result, employees may not be adequately trained or understand their roles and responsibilities.

We recommend that management:

- Follow its policy by conducting annual performance appraisals and creating training plans.
- Update new employee training materials.

Internal Audit

Senior management is responsible for ensuring that regular independent audits are obtained regarding the effectiveness, efficiency and economy of security and internal control procedures, and management's ability to control IT function activities. This work can be accomplished through a combination of both internal and external audits.

The department's internal audit section has not provided assurance regarding controls within the data center, but relies solely on external audits. As a result, management has not received regular feedback regarding the data center's ability to meet operational goals and objectives.

We recommend that internal audit provide periodic reviews of the data center's operations.

Follow-up on Prior Audit Recommendations

During the current audit, we reviewed the department's efforts to implement prior audit recommendations communicated in our reports No. 1999-33 and No. 1994-38, issued October 8, 1999 and December 30, 1994, respectively.

Of the 15 audit recommendations made in the 1999 report, three have been resolved and two partially resolved. Of those recommendations not resolved, six were concerns repeated from our 1994 audit. Those prior recommendations not resolved are discussed in the body of this report.

Objectives, Scope and Methodology

The objective of our audit was to evaluate the adequacy of the Oregon Department of Transportation's general controls at its data center. We also evaluated compliance with applicable laws, rules and regulations pertaining to the operation of information systems.

Our audit work included inquiries of data center personnel, examination of documents related to controls and procedures, and observation of information systems control processes and operations. We performed our fieldwork between March 2001 and August 2001.

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 research, develop, and publicize control objectives and audit guidelines.

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

October 31, 2001

DEPARTMENT OF
TRANSPORTATION

Cathy Pollino, Director
Oregon Audits Division
255 Capitol Street NE, Suite 500
Salem OR 97310

Dear Ms. Pollino:

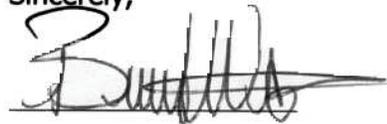
Following is our response to the Secretary of State's draft report, "Data Center General Controls Review" conducted from March 2001 through August 2001.

Thank you for the opportunity to review the Exit Draft audit report. ODOT Information Systems generally agrees with the report contents and appreciates your suggestions and recommendations.

As a leading Information Technology office within the State of Oregon, with a reputation for technology leadership and expertise, strong IT governance structure, high systems availability and proven ability to counteract attacks against our IT environment, we welcome any information that can help us become more successful in our endeavors. In addition to receiving and acting on audit reports from your office and from ODOT Internal Audit Services, we participate actively in continuous improvement, including working with the Gartner Group and other internationally respected organizations.

We value the Audits Division's involvement and recognize the recommendations as representative of industry best practices. ODOT Information Systems is currently working to resolve many of the issues identified in your report. Some of the recommendations will require additional resources to implement. While we are supportive of making necessary improvements, our ability to implement all recommendations may depend on factors such as legislative action, resource availability and policy changes.

Sincerely,



Bruce Warner,
Director



David White,
Chief Information Officer

c:
Mike Marsh, Executive Deputy Director
Drummond Kahn, Chief of Internal Audit Services



555 13th St. NE, Suite 1
Salem, OR 97301-4166
(503) 986-4400
FAX: 986-4072



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: *Nancy L. Young, CISA, CPA* • AUDIT STAFF: *Kelly L. Olson, CPA* • *Virginia Teller* • *Cynthia Hubbard*

ACTING DEPUTY DIRECTOR: *Charles A. Hibner, CPA*

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

Auditing to Protect the Public Interest and Improve Oregon Government

OFFICE OF THE
SECRETARY OF STATE

Bill Bradbury
Secretary of State



AUDITS DIVISION
Cathy Pollino
Director

(503) 986-2255
FAX (503) 378-6767

Auditing for a Better Oregon

The Honorable John Kitzhaber, M.D.
Governor of Oregon
254 State Capitol
Salem, Oregon 97310-4047

Bruce A. Warner, Director
Oregon Department of Transportation
355 Capitol Street NE
Salem, Oregon 97301-3871

The attached report presents the results of our general controls review of the Oregon Department of Transportation data center. General controls protect the environment in which software applications process data. We included a follow up on prior audit findings.

During the review, we found that the data center's general controls could be improved to further protect its equipment and people. Some of these weaknesses were addressed in our prior audit reports No. 1999-33 and No. 1994-38, issued October 8, 1999 and December 30, 1994, respectively. The report includes recommendations intended to improve the department's disaster recovery and contingency planning, physical and logical security, systems development activities, protection from environmental hazards, organization controls, and internal audit coverage.

OREGON AUDITS DIVISION

Bill Bradbury
Secretary of State

Fieldwork Completion Date:
August 23, 2001