

# Oregon Department of Transportation: Data Center General Controls Review Follow Up



Cathy Pollino, State Auditor, Audits Division

Bill Bradbury, Secretary of State

## Secretary of State Audit Report

### Summary

#### PURPOSE

The purpose of this audit was to determine whether the Oregon Department of Transportation resolved findings identified in Audits Division report No. 2001-51, *Oregon Department of Transportation, Data Center General Controls Review* issued in November 2001. That audit was conducted to evaluate the adequacy of general controls in place at the Oregon Department of Transportation data center.

#### RESULTS IN BRIEF

The Oregon Department of Transportation has made some progress in resolving the findings identified during the prior audit. Of 26 findings,

five were resolved, nine were partially resolved, and 12 were not resolved.

#### RECOMMENDATIONS

**We recommend** that the Oregon Department of Transportation management implement the recommendations made for the 21 audit findings that have not been fully resolved within the context of the data center consolidation.

#### AGENCY'S RESPONSE

The Oregon Department of Transportation partially agrees with the findings. The agency's response can be found at the end of the report.

### 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 section consists of six units, one of which is the Technology Management unit. This unit operates the department's data center and provides support related to network and mainframe operations, telecommunications, and wireless communications, among others.

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, 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.

### 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

### Audit Results

We found that the Oregon Department of Transportation Technology Management unit has made some progress in resolving the findings identified during the prior data center general controls audit, Report No. 2001-51. Of the 26 findings, five were resolved, nine were partially resolved, and 12 were not resolved.

During our audit we were aware of the state's initiative to consolidate its data centers and the department's role in that undertaking.

Such transition periods are often accompanied by elevated risks as priorities change and routine controls are often set aside.

**We recommend** that the Oregon Department of Transportation management implement the recommendations made for the 21

findings that have not been fully resolved within the context of the data center consolidation.

### Summary of Prior Audit Findings

This section summarizes the Oregon Department of Transportation’s efforts to resolve prior audit findings included in our report No. 2001-51, *Oregon Department of Transportation: Data Center General Controls Review*.

Prior Audit Findings	Prior Audit Recommendations	Current Status
<b>Ensuring Continuous Service</b>		
<p><b>Disaster Recovery Plan</b></p> <p>Although the department had developed some disaster recovery and contingency plans, the department had not made recovery of its operations a priority. The plans were out of date and elements of these plans were incomplete or missing important information including the following:</p> <ul style="list-style-type: none"> <li>• Various disaster recovery response scenarios from minor to total loss of capability and responses to each, insufficient detail for step-by-step execution.</li> <li>• Detailed lists of equipment and supplies necessary to recover operations.</li> <li>• Written agreements to ensure that vendors will provide expected services.</li> </ul>	<p>We recommended that management make recovery of its operations a priority by fully developing, implementing, and maintaining disaster recovery and contingency plans.</p>	<p><b>Not Resolved.</b> Although the department has completed an Emergency Operations Plan and is in the process of updating its disaster recovery and contingency plans, these plans are still missing key elements as noted in the prior audit.</p>
<p><b>Disaster Recovery Plan Testing</b></p> <p>Tests were last performed in 1996 and recovery team members were not aware of their responsibilities.</p>	<p>We recommended that management conduct periodic testing of those plans and train recovery team members.</p>	<p><b>Not Resolved.</b> Training of staff and testing of the plans are not current.</p>
<p><b>Offsite Storage Location</b></p> <p>The department’s off-site storage facility was not located far enough away from the data center so as not to be affected by the same disaster.</p>	<p>We recommended that management relocate its offsite storage facility to a location that would be less affected by the same disaster.</p>	<p><b>Resolved.</b> The department is now utilizing an off-site storage facility located far enough away from the data center so as not to be affected by the same disaster.</p>

Prior Audit Findings	Prior Audit Recommendations	Current Status
<p><b>Offsite Storage Contents</b></p> <p>The department had not identified items needing to be stored at the off-site facility and those items that have been identified as needing to be stored offsite were not found.</p>	<p>We recommended that management store those items needed for recovery at the offsite facility.</p>	<p><b>Not Resolved.</b> The department has not identified all items needed for recovery.</p>
<b>Physical Access Controls</b>		
<p><b>Data Center Access</b></p> <p>Not all individuals who had access to the data center had 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.</p> <p>In addition, procedures for issuing temporary keycards did not require formal manager approval.</p>	<p>We recommended that management further develop, implement and consistently enforce policies and procedures to limit access to its computer systems, including:</p> <ul style="list-style-type: none"> <li>• Periodic review and confirmation of access privileges,</li> <li>• Formal authorization from data center management to obtain access regardless of the origination, and</li> <li>• Monitoring of access to the data center.</li> </ul> <p><b>We also recommended</b> that management 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.</p>	<p><b>Not Resolved.</b> Department management has not developed or implemented policies and procedures to limit access to its computer system including:</p> <ul style="list-style-type: none"> <li>• Periodic review and confirmation of access privileges,</li> <li>• Formal authorization from data center management to obtain access regardless of origination, and</li> <li>• Monitoring of access to the data center.</li> </ul> <p><b>Not Resolved.</b> Review of access reports for a three-month period showed that 65 percent of those granted access did not utilize their key card to access the data center. According to department management many of these individuals did not have a need for the access.</p>
<p><b>Criminal History Background Checks</b></p> <p>Documentation did not support that all employees and vendors with access to the data center had passed a criminal history background check and procedures for issuing temporary keycards did not require criminal history background checks.</p>	<p>We recommended that management consistently apply its existing procedures for conducting criminal history background checks.</p>	<p><b>Partially Resolved.</b> We selected a sample of 20 employees and found that a criminal history background check had been completed for each employee. However, written procedures for issuing temporary keycards do not require criminal history background checks.</p>
<p><b>Visitor Logs</b></p> <p>Visitor logs were incomplete and not reviewed.</p>	<p>We recommended that management follow its existing procedures for completing visitor logs.</p>	<p><b>Resolved.</b> Visitor logs were completed and according to management, the logs are reviewed every couple of weeks.</p>

Prior Audit Findings	Prior Audit Recommendations	Current Status
<b>Logical Access Controls</b>		
<p style="text-align: center;"><b>System Settings</b></p> <p>Some system parameters were not set in accordance with the department's policy.</p>	<p>We recommended that management set system parameters in accordance with policy.</p>	<p><b>Partially Resolved.</b> The department has not set all system parameters in accordance with policy.</p>
<p style="text-align: center;"><b>Shared User ID</b></p> <p>One user ID allowed access to all system information, was shared among technical support employees, and had conflicting access privileges.</p>	<p>We recommended that management enforce its existing policy and procedures by ensuring all users have a unique ID.</p>	<p><b>Resolved.</b> Management has limited the use of the previously identified shared profile.</p>
<p style="text-align: center;"><b>Access Authorization</b></p> <p>Authorization of access was not always documented. In addition, the Computer Security Unit did not have a complete list of managers or other designees authorized to approve access.</p>	<p>We recommended that management enforce its existing policy and procedures by documenting all requests for access.</p>	<p><b>Partially Resolved.</b> Although the Computer Security Unit has a process to verify a manager authorized access requests, they were unable to provide documentation supporting authorization of access for 4 (12.5%) of 32 sampled users.</p>
<p style="text-align: center;"><b>Periodic Evaluation of Access Rights</b></p> <p>The department did not periodically evaluate its employees' access privileges to ensure that they remained appropriate for current work assignments.</p>	<p>We recommended that management develop and implement additional procedures to require periodic reevaluation of access privileges.</p>	<p><b>Not Resolved.</b> There is no formal process in place requiring periodic reevaluation of access privileges.</p>
<p style="text-align: center;"><b>Data Classification</b></p> <p>The department had 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.</p>	<p>We recommended that management create and maintain a data classification scheme.</p>	<p><b>Not Resolved.</b> The department has not developed a data classification scheme.</p>
<p style="text-align: center;"><b>Incident Handling Procedures</b></p> <p>The department had not developed incident handling and formal escalation procedures to be followed in the event of a security incident.</p>	<p>We recommended that management establish incident handling and escalation procedures.</p>	<p><b>Not Resolved.</b> The department has not established incident handling or escalation procedures.</p>
<p style="text-align: center;"><b>Access Deactivation</b></p> <p>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.</p>	<p>We recommended that management modify its existing policy to require access to be revoked no later than the end of the employee's last workday.</p>	<p><b>Not Resolved.</b> The department's policy allows access to remain activated for up to seven days after employee termination.</p>

Prior Audit Findings	Prior Audit Recommendations	Current Status
<p><b>Password Confidentiality</b></p> <p>Users were not prohibited from sharing their passwords with technical support staff.</p>	<p>We recommended that management modify its existing policy to prohibit employees from sharing their passwords.</p>	<p><b>Resolved.</b> The department’s policy was revised to prohibit employees from sharing passwords.</p>
<p><b>Unrestricted Access</b></p> <p>Technical support employees had unrestricted access to production programs and data, assisted in application program development, and management did not monitor those activities.</p>	<p>We recommended that management limit technical support employees’ access to the production environment and data and monitor those activities.</p>	<p><b>Not Resolved.</b> Access and activities in the production environment have not been limited and management does not monitor those activities.</p>
<p><b>Acquire and Maintain Technology Infrastructure</b></p>		
<p><b>Acquiring and Maintaining System Software and Hardware</b></p> <p>Review of selected purchases made showed that Technology Management 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.</p> <p>Procedures for controlling changes to the system were informal and did not include all of the necessary steps to adequately control changes made. For example, system documentation including the operations manual was not updated or maintained and a quality assurance review was not conducted.</p>	<p>We recommended that management fully develop, document and implement formal methodologies addressing acquiring and maintaining system software and hardware. Those methodologies should include missing steps and deliverables as identified.</p>	<p><b>Partially Resolved.</b> The department has some written procedures in place addressing consideration and documentation of requirements and a formal implementation plan and post implementation review. However, security considerations, documentation of testing, and formal approval prior to move into production are not adequately defined. In addition, while some change management procedures have been documented, management and staff were unable to provide such procedures during the audit. Those procedures lacked detail requiring updating system documentation and quality assurance.</p>
<p><b>Problem Management Procedures</b></p> <p>The department had not developed problem management procedures.</p>	<p>We recommended that management fully develop, document and implement problem management procedures.</p>	<p><b>Partially Resolved.</b> The department has started documenting some procedures including contact persons and reporting times. However, procedures for detection, documentation, logging and resolution remain incomplete.</p>
<p><b>Software Upgrade Policy</b></p> <p>The policy outlining responsibilities and deliverables related to software upgrades was not followed and responsible parties stated that they were not aware such a policy existed.</p>	<p>We recommended management enforce its existing policy when making upgrades.</p>	<p><b>Not Resolved.</b> Since our prior audit, the department revised existing procedures, eliminating important elements, such as creation of testing plans and documentation of testing results.</p>

Prior Audit Findings	Prior Audit Recommendations	Current Status
<p><b>Surplus Equipment</b></p> <p>Equipment was sent to surplus for resale without ensuring all data had been properly erased prior to disposal.</p>	<p>We recommended that management ensure that all data is removed from equipment and other media before sending to surplus.</p>	<p><b>Partially Resolved.</b> Although the department has an automated tool in place intended to remove data from equipment before being sent to surplus, the technical specifications of the tool used are unknown. As such, the department has no assurance that all data has been removed from equipment and other media.</p>
<p><b>Managing Facilities</b></p>		
<p><b>Fire Extinguisher Training</b></p> <p>Data center employees had not received periodic training on how to use fire extinguisher equipment.</p>	<p>We recommended 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.</p>	<p><b>Partially Resolved.</b> Fire extinguisher equipment training was given to data center employees in July 2003. However, there is no policy or procedure in place to require periodic training and no further training is planned.</p>
<p><b>Environmental Monitors</b></p> <p>Procedures were not in place to ensure that all environmental monitors were maintained and working according to specifications and inspections were not documented.</p>	<p>We recommended that management fully develop and implement procedures to ensure environmental monitors are maintained and working as well as documenting inspections.</p>	<p><b>Partially Resolved.</b> Data center staff performs and documents a review of monitors weekly. The department also relies on DAS Facilities to ensure environmental controls are maintained. However, there are no documented procedures requiring this review or explaining the reliance on DAS Facilities.</p>
<p><b>Response Scenarios</b></p> <p>Documented procedures did not adequately describe expected response scenarios for various environmental emergencies.</p>	<p>We recommended that management fully develop and implement procedures including expected response scenarios for various environmental emergencies.</p>	<p><b>Not Resolved.</b> While there have been some additions to the Emergency Operations Plan noting potential environmental emergencies, the plan is insufficient as it does not define specific response scenarios.</p>

Prior Audit Findings	Prior Audit Recommendations	Current Status
<b>Organization and Relationships</b>		
<p><b>Annual Performance Evaluations and Training Plans</b></p> <p>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.</p>	<p>We recommended that management follow its policy by conducting annual performance appraisals and creating training plans.</p>	<p><b>Partially Resolved.</b> We reviewed 10 employees to determine if performance appraisals and training plans were completed annually, in accordance with the department's policy. We found that performance evaluations were completed for all 10, however training plans were only completed for 3 of the 10.</p>
<p><b>New Employee Training Materials</b></p> <p>The data center's new employee training materials were outdated.</p>	<p>We recommended that management update new employee training materials.</p>	<p><b>Resolved.</b> The new-employee training manual was updated as of March 2004.</p>
<b>Internal Audit</b>		
<p><b>Internal Audits</b></p> <p>The department's internal audit section had not provided assurance regarding controls within the data center, but relied solely on external audits.</p>	<p>We recommended that internal audit provide periodic reviews of the data center's operations.</p>	<p><b>Not Resolved.</b> While consideration of Information Systems is part of the risk assessment process for the Internal Audit Services, periodic reviews of the data center operations are not conducted.</p>

**Objectives, Scope and Methodology**

The objective of our audit was to determine whether the Oregon Department of Transportation resolved findings identified in our report No. 2001-51, *Oregon Department of Transportation, Data Center General Controls Review* issued in November 2001. The audit was conducted to evaluate the adequacy of the Oregon Department of Transportation's general controls in place at the Oregon Department of Transportation's data center. We also considered applicable laws, rules and regulations pertaining to our audit objective. 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 and August 2004.

During our audit, 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. ITGI 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.

## Oregon Department of Transportation's Response to the Audit Report

Following is our response to the Secretary of State's report, *Data Center General Controls Review Follow Up* conducted from March through August 2004.

Thank you for the opportunity to review the report. ODOT Information Systems partially agrees with the report contents. In particular, ODOT does not believe that this audit reflects or recognizes the vast amount of procedural and operational changes ODOT has made based on the original audit findings. As a result of the original audit findings two years ago, ODOT has implemented operational changes, conducted training courses, and implemented new management systems to address the shortcomings found in the original audit. ODOT does not see that these changes have been considered in the audit findings. Faced with fiscal challenges, ODOT has been able to excel in the areas of service delivery and customer satisfaction. In a time of forced employee reduction, ODOT IS has maintained superior system performance and implemented numerous procedural changes as a result of the audit findings.

ODOT recently hired a new Chief information Officer, Ben Berry, who has reviewed the audit findings as well as the measures taken by ODOT IS since the audit field work was completed. His current review of the items identified is attached with this memorandum. He is committed to addressing the unresolved issues identified in your report, understanding that some of the recommendations will require additional resources to implement and some will be addressed through Computer and Networking Infrastructure Consolidation and other statewide initiatives.

Our Information Technology office has a reputation for technology leadership and expertise, high systems availability and proven ability to counteract attacks against our IT environment. We welcome any information that can help us be more successful in our endeavors.

### ODOT CIO Review of SOS Data Center Controls Audit

Ben Berry CIO  
November 22, 2004

	Prior Audit Findings	SOS Audit	ODOT Status *		
			Resolved	Partially Resolved	Needs Work
1	Disaster Recovery Plan	Not Resolved			
2	Disaster Recovery Plan Testing	Not Resolved			
3	Offsite Storage Location	Resolved			
4	Offsite Storage Contents	Not Resolved			
5	Data Center Access	Not Resolved			
6	Criminal History Background Checks	Partially Resolved			
7	Visitor Logs	Resolved			
8	System Settings	Partially Resolved			
9	Shared User ID	Resolved			
10	Access Authorization	Partially Resolved			
11	Periodic Evaluation of Access Rights	Not Resolved			
12	Data Classification	Not Resolved			
13	Incident Handling Procedures	Not Resolved			
14	Access Deactivation	Not Resolved			
15	Password Confidentiality	Resolved			
16	Unrestricted Access	Not Resolved			
17	Acquiring and Maintaining System	Partially Resolved			
18	Problem Management Procedures	Partially Resolved			
19	Software Upgrade Policy	Not Resolved			
20	Surplus Equipment	Partially Resolved			
21	Fire Extinguisher Training	Partially Resolved			
22	Environmental Monitors	Partially Resolved			
23	Response Scenarios	Not Resolved			
24	Annual Performance Evaluations and Training Plans	Partially Resolved			
25	New Employee Training Materials	Resolved			
26	Internal Audits	Not Resolved			
			9	16	1

(Auditor's Footnote)

\* ODOT's current status differs from the audit results in 13 of the 26 items listed above. ODOT's status is based on actions taken or proposed actions to be taken subsequent to the audit period and not what was completed since the audit.





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: *Nancy L. Young, CPA, CISA, CFE*

AUDIT STAFF: *Shandi C. Frederickson, CPA  
Darrin D. Hotrum, CISA  
Chris Knutson*

DEPUTY STATE AUDITOR: *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.*

*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*