

AUDIT REPORT

Department of Administrative Services: 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 Department of Administrative Services 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, and independent audit. We included a follow up of prior audit findings.

RESULTS IN BRIEF

The Department of Administrative Services data center's general controls could be improved to further protect its equipment and people. Some of the weaknesses noted were addressed in a prior audit report.

RECOMMENDATIONS

We recommend that management:

- Make disaster recovery and contingency planning a priority to ensure 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.
- Provide periodic internal audit reviews of the data center.

AGENCY RESPONSE

The Department of Administrative Services generally agrees with the recommendations.

Background

The Department of Administrative Services (department) is the central administrative agency of state government. The department is responsible for improving the efficient and effective use of state resources through the provision of statewide information systems and networks to facilitate the reliable exchange of information and applied technology. The department's Information Resources Management Division (division) operates the department's data center in addition to the state's voice, video and data networks. The division covers its operating costs by charging agencies for services provided.

The data center operates and maintains the mainframe computer system used to process transactions

for statewide applications such as the state's accounting, payroll, and personnel systems.

On February 26, 1999, the governor signed Executive Order EO 99-05 directing the operational alignment of the Oregon Department of Transportation's 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, 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 1999, 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 off-site 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 items needing to be stored at the off-site facility.

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 off-site storage facility to a location that would be less affected by the same disaster and identifying and storing those items needed for recovery at the off-site facility.

***Agency Response:** We agree and are currently in the process of developing an RFP [Request for Proposal] to select a vendor that will provide disaster recovery services to the GGDC [General Government Data Center], ODOT, DHS, and Department of Revenue. Once a vendor has been selected, GGDC staff will work with the vendor to develop a contingency plan to restore any service(s) that may be lost. Contingency plan will also cover localized emergency situations not requiring services provided by disaster recovery vendor.*

We agree that it is important to test recovery plans. The contract with the provider of disaster recovery services will provide for two on-site tests per year. During these tests GGDC staff will be testing detail recovery procedures developed for all platforms used by the data center. Following the test, we will conduct "Lessons Learned" sessions to get information on what worked and didn't work. Recovery plans and test plans will be updated accordingly.

We agree. GGDC will initiate a search to find a new location for off-site storage that meets requirements for security and accessibility.

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 is subject to a criminal history background check. 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 date. One vendor's keycard was still active almost one year after terminating services.
- 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 30 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.

As a result, management is less able to protect its data and systems from unauthorized use. These weaknesses exist because management's periodic review and confirmation of access privileges are

limited to only data center staff. Furthermore, other agency management can authorize and issue keycards to the data center without the department's authorization and knowledge. In addition, management does not ensure that documentation is maintained supporting criminal history background checks and is completed for visitors to the data center. Finally, although policy describes procedures for deactivating keycards, it does not require that deactivation be made in a timely manner.

We recommend that management modify its existing procedures to require:

- Periodic review and confirmation of access privileges for all individuals having access to the data center.
- Review and approval of all requests for access to the data center regardless of origination.
- Keycards be deactivated no later than the employee's or vendor's last workday.

We also recommend that management immediately revoke keycard access for those individuals who do not have a demonstrated need for such access and for those the department did not authorize; maintain documentation supporting criminal history background checks; and ensure visitor logs are complete and reviewed.

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 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 data center and submit

requests to the data center's management.

- Establish keycard access to the data center only upon formal approval by the data center management.

Agency Response: *We agree existing procedures should be modified. IRMD [Information Resources Management Division] will develop criteria to determine whether an individual has a legitimate need to access the data center. A procedure will be developed to review and update data center access privileges on a semi-annual basis.*

We agree. Appropriate procedures will be developed by IRMD and the Facilities Division that will give GGDC management approval rights over access to the data center.

We agree. Appropriate procedures will be developed or modified by IRMD to ensure timely notification to GGDC and Facilities Division when employees and vendors no longer need access to the data center.

We agree existing procedures should be modified. IRMD will develop criteria to determine whether an individual has a legitimate need to access the data center. GGDC management will request from Facilities Division a current list of individuals who currently have access to the data center. This list will be reviewed based on the established criteria and a list will be produced of those individuals who don't need data center access. The list will be sent to Facilities Division to be processed. Procedures will be modified to ensure that e-mails for background approvals are retained in employee's file. Also, procedures will be modified to ensure data center access logs are reviewed by a GGDC manager on a weekly basis.

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, policy requires users to be given a unique ID and system parameters are set to force periodic password changes. In addition, employees are to read and sign a Computer Security User Declaration statement acknowledging their understanding of the department's security policies.

During our review, we found that management does not always ensure that its policies are followed. For example, one user ID is shared among technical support employees and, thus, management is less able to determine who initiated actions with that ID. In addition, the password to this ID has not been changed in one year, as the system parameter forcing the change has been overridden.

Some procedures are not adequate and should be modified, including the following:

- The department requires only new employees to read and sign the policy acknowledgment statement even though the policy is applicable to all department employees.
- Procedures do not ensure access is deactivated in a timely manner. One of five terminated user accounts reviewed remained active after the employee's termination.
- Although policy requires users to keep their passwords confidential at all times, the policy authorizes sharing passwords at the direction of a manager.

Management has not established some necessary procedures. For example:

- The data center management does not periodically evaluate its employees' access privileges to ensure that they remain appropriate for current work assignments.
- The department has not developed incident handling and formal escalation procedures to be followed in the event of a security incident.

Finally, the department's organizational structure does not always support adequate separation of sensitive functions according to best practices. Production control staff performs operator functions and technical support staff may assist in application program development and support. Furthermore, technical support employees have unrestricted access to production programs and data, management does not monitor those activities, and one user ID reviewed has conflicting access privileges.

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 by ensuring that all users have a unique ID and all passwords are periodically changed.
- Modify its existing policy to require all employees to sign the policy acknowledgment statement regardless of their hire date, access be revoked no later than the end of an employee's last workday, and for users to never share their passwords.
- Develop and implement additional procedures to require

periodic reevaluation of access rights, and create and establish incident handling and escalation procedures.

- Reassign production control, operations, and technical support staff activities to provide better separation of these critical functions. In addition, limit technical support employees access to the production environment and data, monitor those activities and remove conflicting access privileges from ID's.

Agency Response: *We agree. Mainframe RACF [(IBM's) Resource Access Control Facility] requires passwords to be changed every 90 days and conform to current standard. Open Systems will implement software in 2002 that will ensure passwords conform to standards and be changed every 90 days.*

We believe existing DAS IT [Information Technology] Policy requires employees to sign the employee statement. We agree that all current GGDC employees and contractors should sign the current acknowledgment statement. Appropriate policies will be developed or modified by IRMD to ensure timely notification to GGDC and Facilities Division when employees and vendors no longer need system access.

We agree. GGDC management will develop and implement procedures to manage access rights granted to GGDC employees and contractors. DAS Policy 107-01-080 contains an incident response procedure on page 11. However, the position that incidents are to be reported to, the IT Security Manager in SP&R [Strategic Planning and Review], is vacant. GGDC will develop an interim procedure until the position is filled.

We understand the concern and will review existing practices with the goal of ensuring better separation of duties. The nature of

the work and responsibilities of technical support staff require that they be granted wide access rights in order to perform regular job duties and handle emergency situations that may occur at night and on weekends. GGDC management will establish guidelines to ensure that these access rights are appropriate, reasonable, and commensurate with requirements to restore failed services in a timely manner.

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 data center 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 shows that the data center may not complete all necessary steps or phases. For example, staff could not demonstrate to what extent feasibility studies had been conducted and equipment had been tested before purchasing.
- Procedures for controlling changes to the system do not include all of the necessary steps to adequately control changes made. For example, system documentation including the operations manual and version listings are not updated or maintained. In addition, quality assurance, and implementation

and post implementation reviews are not conducted.

- Procedures do not address processes to ensure that all data has been properly erased prior to disposing equipment and media.
- 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.

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, ensuring that all data is removed from equipment and other media prior to disposal, and problem management procedures.

Agency Response: We agree that the GGDC should develop and implement a life cycle approach to major hardware and system software acquisitions. Additionally, the GGDC will apply a project management discipline to acquisitions and upgrades. Supporting procedures will be developed to address equipment disposal issues. Problem management will be addressed as a GGDC-wide issue covering appropriate aspects of systems operations, technical support, and customer support.

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 responsibility for 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 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 that environmental monitors are maintained and working as well as documenting inspections.
- Expected response scenarios for various environmental emergencies.

Agency Response: We agree. An emergency equipment training plan will be developed. Training sessions

will be scheduled at regular intervals for GGDC operations staff.

We agree. Procedures will be developed to ensure regular monitoring of environmental monitors, logging of observed measurements, and reporting of abnormal readings to GGDC management.

We agree. Environmental emergency responses will be documented and included in the GGDC Contingency Plan.

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 information technology 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.

Agency Response: We agree. IRMD will request Internal Audit to conduct periodic reviews.

Follow up on Prior Audit Recommendations

During the current audit, we reviewed the department's efforts to implement prior audit recommendations communicated in our report No. 1998-39, issued on December 27, 1998.

Of the eight audit recommendations made in the 1998

report, one has been resolved and two partially resolved. Those prior recommendations not fully resolved are discussed in the body of this report or as follows:

- Network Operations Center fully develop and maintain a disaster recovery and contingency plan. Partially resolved.
- IRMD and DAS Facilities Division determine appropriate measures for improving physical security of the data center. Not resolved.

Agency Response: *We agree. NOC management is working to complete its disaster recovery and contingency plan.*

We agree that this has not been resolved. As mentioned in other responses in this document, IRMD

will work with the Facilities Division to develop procedures that ensure only authorized individuals have access to the data center.

Objectives, Scope and Methodology

The objective of our audit was to evaluate the adequacy of the Department of Administrative Services 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.

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*

DEPUTY DIRECTOR: *Charles Hibner, CPA*

The courtesies and cooperation extended by the officials and staff of the Department of Administrative Services 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
Catherine E. 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

Michael Greenfield, Director
Department of Administrative Services
155 Cottage Street NE
Salem, Oregon 97301

The attached report presents the results of our general controls review of the Department of Administrative Services 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 report No. 1998-39, issued on December 27, 1998. 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, and internal audit coverage.

OREGON AUDITS DIVISION

Bill Bradbury
Secretary of State

Fieldwork Completion Date:
August 23, 2001