



Department of Administrative Services: Data Center General Controls Review Follow Up

Summary

Cathy Pollino, State Auditor, Audits Division

Bill Bradbury, Secretary of State

Secretary of State Audit Report

PURPOSE

The purpose of this audit was to determine whether the Department of Administrative Services implemented recommendations made in Audits Division report No. 2001-50, *Department of Administrative Services, Data Center General Controls* issued in November 2001. That audit was conducted to evaluate the adequacy of general controls in place at the Department of Administrative Services General Government Data Center (GGDC).

RESULTS IN BRIEF

The Department of Administrative Services GGDC has made some progress in implementing the recommendations made during the prior audit. Of 25 recommendations, seven were resolved, three were partially resolved, and 15 were not resolved.

RECOMMENDATIONS

We recommend that the Department of Administrative Services management implement the 18 audit recommendations that have not been fully resolved within the context of the Computing and Networking Infrastructure Consolidation (CNIC) Initiative.

We also recommend that the Department of Administrative Services GGDC management work with the Facilities Division to become designated as a High Security Access Area.

AGENCY'S RESPONSE

The Department of Administrative Services generally agrees with the findings in the original audit report and follow-up report.

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 (IRMD) operates the department's General Government Data Center (GGDC) in addition to the state's voice, video and data networks. The division covers its operating costs by charging agencies for services provided.

The GGDC operates and maintains the mainframe computer system used to process transactions for statewide applications such as the state's accounting, payroll, and personnel systems.

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

We found that the Department of Administrative Services IRMD’s management has made some progress in implementing the recommendations made during the prior data center general controls audit, Report No. 2001-50. Of the 25 recommendations made, seven were resolved, three were partially resolved, and 15 were not resolved.

During our audit we were aware of the state’s Computing and Networking Infrastructure Consolidation (CNIC) 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 set aside.

We recommend that the Department of Administrative

Services management implement the 18 audit recommendations that have not been fully resolved within the context of the CNIC Initiative.

We also recommend that the Department of Administrative Services GGDC management work with the Facilities Division to implement the new access control policy and become designated as a High Security Access Area.

Summary of Prior Audit Findings

This section summarizes the Department of Administrative Services’ efforts to resolve prior audit findings included in our report No. 2001-50, *Department of Administrative Services: Data Center General Controls Review*

Prior Audit Findings	Prior Audit Recommendations	Current Status
Ensuring Continuous Service		
<p>Disaster Recovery Plan</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"> - 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. 	<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>Not Resolved. Since the prior audit the GGDC has hired a new hot site disaster recovery contractor to provide recovery services. However, the GGDC’s disaster recovery and contingency plans in place during the prior audit are no longer in place and management has yet to develop any new plans.</p>
<p>Disaster Recovery Plan Testing</p> <p>Tests of the disaster recovery plan were last performed in 1999, 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>Not Resolved. The GGDC currently has no disaster recovery plan in place.</p>
<p>Off-Site Storage Location</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 off-site storage facility to a location that would be less affected by the same disaster.</p>	<p>Resolved. The GGDC is now utilizing an off-site storage facility located far enough away from the GGDC so as not to be affected by the same disaster.</p>

Prior Audit Findings	Prior Audit Recommendations	Current Status
<p>Off-Site Storage Contents</p> <p>The department had not identified items needing to be stored at the off-site facility.</p>	<p>We recommended that management identify and store those items needed for recovery at the off-site facility.</p>	<p>Not Resolved. The data center has not identified all items needed for recovery.</p>
<p>Agency's Response</p> <p>Disaster Recovery Plan GGDC is currently in the process of setting up an October 2004 disaster recovery test. When the date is set up, the data center will be working collaboratively with Sungard on a disaster recovery plan. GGDC expects to have a disaster recovery plan in place by November 30, 2004.</p> <p>Disaster Recovery Plan Testing Since the 1999 audit, the data center has had a disaster recovery test in June 2001. The disaster recovery test, with plan included, has been received by SOS Audits. The data center is in the process of setting up a date with Sungard for a test in October 2004. GGDC plans to have a disaster recovery plan in place by November 30, 2004.</p> <p>Off-Site Storage Contents GGDC will have a new disaster recovery kit in place by November 30, 2004, based on the disaster recovery plan developed. While our current kit may not contain all the items needed for a full recovery of production systems in general, we store all items needed for full recovery of production systems that customers have identified as production data at the off-site facility. GGDC is in the process of formalizing its documentation process. In addition, CNIC will address this issue.</p>		
Prior Audit Findings	Prior Audit Recommendations	Current Status
<p>Physical Access Controls</p>		
<p>Data Center Access</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 30 percent actually obtained access to the data center during the period reviewed.</p> <p>These weaknesses exist because other agency management can authorize and issue keycards to the data center without the department's authorization and knowledge.</p>	<p>We recommended that management modify its existing procedures to require:</p> <ul style="list-style-type: none"> - 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. <p>We also recommended that management immediately revoke keycard access for those individuals who did not have a demonstrated need for such access and for those the department did not authorize.</p>	<p>Not Resolved. Although the GGDC performed a review of access in October 2003, management has not modified their procedures to ensure that such a review is performed periodically. In addition, evidence of managerial approval did not exist for 25 out of 25 sampled personnel who had key card access to the data center. Review of access reports for a three-month period shows that 58 percent of those granted access did not utilize their key card to access the data center. As such, we conclude that those individuals do not have an apparent need for the access granted.</p> <p>Since our last audit, the department's Facilities Division developed a new policy that would allow a data center to become designated as a High Security Access Area. This designation would prevent other agency management from authorizing and issuing keycards to a data center without the data center management's authorization and knowledge. However at the time of our audit, the GGDC management had not</p>

Prior Audit Findings	Prior Audit Recommendations	Current Status
		taken the necessary steps to take advantage of that new policy.
<p>Key Card Deactivation 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.</p>	<p>We recommended that management modify its existing procedures to require keycards be deactivated no later than the employee's or vendor's last workday.</p>	<p>Partially Resolved. Although the procedure has not been modified, we tested five terminated employees and determined that they had their keycards deactivated timely. We did, however, identify one employee outside of the five employees tested who terminated employment in 2001 but continued to have active keycard access at the time of our current review.</p>
<p>Documentation of Background Checks Documentation did not support that all employees and vendors with access to the data center had passed a criminal history background check.</p>	<p>We recommended that management maintain documentation supporting criminal history background checks.</p>	<p>Not Resolved. Documentation of a criminal history background check was not available for 13 out of the 25 (52%) sampled employees.</p>
<p>Visitor Logs Visitor logs were incomplete and not reviewed.</p>	<p>We recommended that management ensure visitor logs were complete and reviewed.</p>	<p>Not Resolved. Visitor logs continue to be incomplete and reviews are not documented.</p>

Agency's Response

Data Center Access

GGDC procedures are being developed to ensure periodic reviews. Completion date is November 30, 2004.

This was previously managed by LEDES (Law Enforcement Data System). In 2001, IRMD and Facilities revised their written procedures to include the requirement that reviews be conducted periodically. IRMD management will review procedures with appropriate staff to ensure reviews are conducted. Access to the data center requires GGDC management to complete a different form than the standard DAS access form. Facilities management will review procedures with staff to ensure the correct form is received prior to granting access to the data center.

Key Card Deactivation

GGDC follows a procedure put in place by IRMD Administrative staff. For a terminating IRMD employee, a checklist is followed with tasks that need to be completed on the last day of employment. One of the tasks includes having the employee return their keycard to GGDC management. In addition, IRMD administrative staff notifies DAS Facilities to deactivate the keycard access. The employee that was found still activated left state service before this process was implemented.

GGDC management is currently conducting a subsequent review of access to ensure that no more instances of separated employee access exist.

Documentation of Background Checks

IRMD is currently waiting for DAS Personnel to approve/finalize a security policy and the process to follow on criminal background checks.

Criminal history background checks for the sampled employees were performed by LEDES. GGDC does not know why LEDES was unable to produce documentation for 13 of the sampled employees. Since LEDES is no longer conducting criminal history background checks for GGDC, IRMD managers are working with DAS Operations management to develop and implement procedures for conducting criminal background checks for the department. These procedures should be in place and fully implemented by December 31, 2004.

Visitor Logs

GGDC implemented a weekly management review of the logs in mid-August 2004 with a computer operations team lead following-up at the end of each day on incomplete entries. Management review of the log is conducted weekly.

Prior Audit Findings	Prior Audit Recommendations	Current Status
Logical Access Controls		
<p>Shared User ID</p> <p>During our review, we found that management did not always ensure that its policies were followed. For example, one user ID was shared among several employees and the password to this ID had not been changed in one year.</p>	<p>We recommended that management enforce its existing policy by ensuring that all users have a unique ID and all passwords are periodically changed.</p>	<p>Resolved. Management has limited the use of the previously identified shared profile and testing shows that forced password changes are required for all individual users.</p>
<p>Policy Acknowledgment Statement</p> <p>The department required only new employees to read and sign the policy acknowledgment statement even though the policy was applicable to all department employees.</p>	<p>We recommended that management modify its existing policy to require all employees to sign the policy acknowledgment statement regardless of their hire date.</p>	<p>Resolved. We tested a sample of 10 employees and found that all had signed the policy acknowledgment statement.</p>
<p>Access Deactivation</p> <p>Procedures did not ensure access was deactivated in a timely manner. One of five terminated user accounts reviewed remained active after the employee's termination.</p>	<p>We recommended that management modify its existing policy to require access be revoked no later than the end of an employee's last workday.</p>	<p>Not Resolved. The policy has not been modified. In addition, access for one out of seven terminated user accounts reviewed remained active for seven days after the employee's termination.</p>
<p>Password Confidentiality</p> <p>Although policy required users to keep their passwords confidential at all times, the policy authorized sharing passwords at the direction of a manager.</p>	<p>We recommended that management modify its existing policy to require users to never share passwords.</p>	<p>Not Resolved. The policy has not been modified.</p>
<p>Periodic Evaluation of Access Rights</p> <p>The data center management 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 rights.</p>	<p>Not Resolved. Although the GGDC has some informal procedures to review access privileges upon certain events, these procedures are undocumented and are not sufficient to ensure a periodic reevaluation of all access rights.</p>
<p>Incident Handling Procedures</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 create and establish incident handling and escalation procedures.</p>	<p>Not Resolved. Although management has established incident handling and escalation procedures addressing cyber security incidents such as attempts to gain unauthorized access to a system or data and denial of service attacks, these procedures are missing key elements including:</p> <ul style="list-style-type: none"> - Detailed steps for detection, initiation, response, recovery, closure, and post-incident review. - Assignment of roles and responsibilities for detection, recovery and closure of security incidents.

Prior Audit Findings	Prior Audit Recommendations	Current Status
		In addition, time frames for response to various severity levels are incomplete.
<p>Organizational Structure</p> <p>The department's organizational structure did not always support adequate separation of sensitive functions according to best practices. Production control staff performed operator functions and technical support staff may have assisted in application program development and support.</p>	<p>We recommended that management reassign production control, operations, and technical support staff activities to provide better separation of those critical functions.</p>	<p>Resolved. Production control, operations, and technical support staff activities have been reassigned to better separate critical functions.</p>
<p>Unrestricted Access</p> <p>Technical support employees had unrestricted access to production programs and data, 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>Not Resolved. Systems analysts continue to have the ability to make programming changes, test those changes, and move the changes into the production environment. Furthermore, management does not monitor those activities.</p>
<p>Conflicting Access Privileges</p> <p>One user ID reviewed had conflicting access privileges.</p>	<p>We recommended that management remove conflicting access privileges from ID's.</p>	<p>Resolved. Conflicting access privileges have been removed from the user identified in the previous audit.</p>

Agency's Response

Access Deactivation

GGDC does not have control of when Personnel functions from different agencies update P.A.s (Personnel Actions) on their terminating employees. The day that a P.A. is issued for an employee termination, a revoke is issued on that person's RACF id. Also, P.C. user accounts must be terminated by the TSC (Technology Support Center). As part of a defined check-off list, a supervisor notifies TSC of when an employee is terminating and requests their user account be inactivated.

GGDC submits a personnel action request to the DAS Personnel Office when an employee terminates employment from the department. The same day the personnel action is issued, access is revoked. The current policy states access should be revoked no later than the end of the employee's last workday.

Password Confidentiality

GGDC agrees with the SOS Audit that the DAS security policy must be revised removing this language.

The Cyber Security unit within IRMD is currently revising all security policies and procedures, in conjunction with CNIC activities. The language authorizing sharing of passwords will be removed. Completion is planned for January 2005.

Periodic Evaluation of Access Rights

IRMD will review employee access privileges at the following trigger events: as position descriptions change, when the organizational structure changes, or at the time annual performance evaluations are conducted. The Technology Support Center is responsible for monitoring access for IRMD. A formal policy will be in place by September 1, 2004.

Incident Handling Procedures

Although not resolved, Cyber-Security is working on this issue.

The Cyber Security unit of IRMD is currently developing procedures related to incident handling, including specifics. The procedures are expected to be in place no later than December 31, 2004.

(Continued next page)

Agency's Response (continued)

Unrestricted Access

In reviewing the COBIT (Control Objectives for Information and Related Technology) System Software Installation Control Objective with SOS Audits and COBIT personnel, GGDC will not be able to meet the requirements of using one set of System Software analysts that install and test software changes and another set of System Software analysts that move the software into production. COBIT personnel acknowledged that although this is the ideal goal, that for the vast majority of shops this is not practical, given the cost in FTE (Full Time Equivalent) to achieve. GGDC agrees with COBIT that the risk is mitigated by having change control practices in place and management approval of the moves into production. We currently are doing so.

COBIT requires compensating controls be in place when the same personnel are used for installing and testing software changes and moving data into production. GGDC has change control practices in place and requires management approval for all moves into production. Documentation is maintained related to all change activity and is available for review. While it would be ideal to have separate employees perform these functions, staffing limitations require GGDC to implement compensating controls.

Prior Audit Findings	Prior Audit Recommendations	Current Status
Acquire and Maintain Technology Infrastructure		
<p>Purchasing Methodology</p> <p>Review of selected purchases showed 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.</p>	<p>We recommended that management fully develop, document and implement formal methodologies addressing system software and hardware. Those methodologies should include missing steps and deliverables as identified.</p>	<p>Partially Resolved. The GGDC has developed some written procedures for acquiring technology infrastructure and during testing of purchases we found that a feasibility study was included in acquisition procedures. However, some key elements are missing or not adequately defined, including:</p> <ul style="list-style-type: none"> - Testing and implementation steps are not adequately addressed. - Purchases identified within the GGDC costing under \$25,000 are not supported by the formal methodology.
<p>Change Management</p> <p>Procedures for controlling changes to the system did not include all of the necessary steps to adequately control changes made. For example, system documentation including the operations manual and version listings were not updated or maintained. In addition, quality assurance, and implementation and post implementation reviews were not conducted.</p>	<p>We recommended that management fully develop, document and implement formal methodologies addressing system software and hardware. Those methodologies should include missing steps and deliverables as identified.</p>	<p>Not Resolved. The change management process has not changed.</p>
<p>Media Disposal</p> <p>Procedures did not address processes to ensure that all data had been properly erased prior to disposing equipment and media.</p>	<p>We recommended that management develop methodologies ensuring that all data is removed from equipment and other media prior to disposal.</p>	<p>Partially Resolved. Although management has developed some procedures for disposing of equipment and media, these procedures are informal.</p>
<p>Problem Management</p> <p>Problem management procedures did not exist.</p>	<p>We recommended that management develop problem management procedures.</p>	<p>Resolved. Problem management procedures have been developed.</p>

Agency's Response

Purchasing Methodology

All technology infrastructure investments require advance approval from the State CIO (Chief Information Officer), based on a compelling business case. Additionally, GGDC follows the formal process established by DAS SPO (State Procurement Office) on all purchases, and follows the vendors' documented implementation steps on all vendor supplied operating software.

Change Management

Ideally, GGDC agrees with the concept. As discussed in Change Management, above, GGDC, and most mainframe shops do not have the FTE to follow this process. This was acknowledged in an email sent by a COBIT representative. A formal Change Management procedure within IRMD mitigates the risk of not having more FTE.

The change management process has changed. Since September 2003, the change management process is monitored by IRMD's Technology Support Center (TSC). Very detailed records are maintained by TSC.

Media Disposal

GGDC agrees. A procedure will be added to the Standard Operation Procedure Manual. No later than November 30, 2004.

Prior Audit Findings	Prior Audit Recommendations	Current Status
Managing Facilities		
<p>Emergency Equipment Training 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>Not Resolved. Since our last audit, some training on the use of fire extinguishers has occurred. However, the GGDC has no plans for future training, and has developed no procedures to ensure that training occurs.</p>
<p>Environmental Monitors 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 that environmental monitors are maintained and working as well as documenting inspections.</p>	<p>Resolved. The GGDC relies on DAS Facilities to ensure environmental controls are maintained. GGDC operators are monitoring temperature and humidity gauges. The GGDC also maintains documentation pertaining to reviews of the fire suppression systems.</p>
<p>Environmental Response Scenarios 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>Not Resolved. While some emergency procedures exist to ensure the safety of personnel, they are not sufficient to ensure that personnel are aware of actions to take to protect GGDC systems under various environmental emergencies.</p>

Agency's Response

Emergency Equipment Training

GGDC acknowledges that policies and procedures are not in place for periodic training. The policies and procedures will be defined within the scope of CNIC. Computer room personnel have received extinguisher training. These employees work in the environment most likely to use an extinguisher. They have also received internal Halon Training.

IRMD is working to ensure all employees receive training on the use of fire extinguishers. Training will be conducted for all new hires and the training repeated when annual performance evaluations are conducted.

(continued next page)

Agency’s Response (continued)

Environmental Response Scenarios

The Cyber Security unit of IRMD is currently revising all security policies and procedures, some of which are triggered by environmental emergencies. They expect to have these revisions completed for environmental emergencies by the end of October 2004.

Comprehensive environmental emergency response plans for the state’s central data center will be developed as part of the CNIC project. Working with application and data owners, GGDC management will develop basic interim environmental response procedures by December 1, 2004.

Prior Audit Findings	Prior Audit Recommendations	Current Status
Internal Audit		
<p>Internal Reviews of Data Center 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>Not Resolved. The internal audit section has not performed a review of GGDC operations, and currently has no specific plans to do so.</p>
<p>Agency’s Response</p> <p>Internal Reviews of Data Center <i>The DAS Internal Audit section performs an annual risk assessment that includes GGDC activities. During the risk assessment process, GGDC controls are reviewed and a risk level is assigned. DAS management is currently contracting with vendors for more specific audit work within IRMD.</i></p>		

Objectives, Scope and Methodology

The objective of our audit was to determine whether the Department of Administrative Services implemented recommendations made in our report No. 2001-50, *Department of Administrative Services, Data Center General Controls* issued in November 2001. That audit was conducted to evaluate the adequacy of general controls in place at the Department of Administrative Services GGDC.

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. We performed our fieldwork between March 2004 and June 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.



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
Erika A. Ungern, CISA
Jessica E. Wicklund*

DEPUTY STATE AUDITOR: *Charles A. Hibner, CPA*

The courtesies and cooperation extended by the officials and staff of the Department of Administrative Services 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*