

Secretary of State
AUDIT REPORT

Department of Administrative Services (DAS):
Computer Center General Controls Review

Phil Keisling, Secretary of State
John Lattimer, Director, Audits Division

Summary

PURPOSE

The objective of our audit was to evaluate the adequacy of general controls in place at the Department of Administrative Services (DAS) Information Resources Management Division's (IRMD) general government data center. General controls are those controls that protect the environment in which software applications process. We reviewed control procedures relating to physical security, access, backup, contingency planning, system and program changes, operations, and other organizational responsibilities. We also included a follow-up of our prior audit findings and a review of IRMD's efforts to ensure year 2000 compliance of the data center.

BACKGROUND

Within the data center, IRMD operates and maintains the mainframe computer system used to process transactions for statewide applications such as the Statewide Financial Management System (SFMS) and the Oregon State Payroll System (OSPS). The data center also contracts to provide computer services to non-state agencies such as cities and counties. Those services includes processing critical transactions such as queries of the state's Law Enforcement Data System (LEDS). In addition, IRMD maintains the state's wide area network.

RESULTS IN BRIEF

We identified weakness that, if corrected could improve access controls, physical security, internal audit coverage,

disaster recovery and contingency planning, and processes to ensure the data center will be year 2000 compliant.

RECOMMENDATIONS

Priority Items

- Resolve identified security issues and evaluate the adequacy of the current computer security configuration.
- Evaluate employees' access rights, review security logs, and adopt procedures for resolving incidents on an escalating basis.
- Escort visitors in the data center and maintain a visitor's log.
- Review and adjust physical security policies and procedures to ensure adequate protection for the data center and its employees.
- Provide for increased internal audit coverage of data center operations and resources.
- Develop a disaster recovery and contingency plan for network operations and perform on-going and regular disaster recovery training.
- Develop and document a comprehensive plan to assess, test, and monitor year 2000 remediation efforts.

AGENCY RESPONSE

The Department of Administrative Services generally agrees with the recommendations.

BACKGROUND

The Department of Administrative Services (DAS) Information Resources Management Division's (IRMD) operates under the authority of Oregon Revised Statutes 291.034 and 291.038. These statutes authorize DAS to provide technical services to state agencies for data processing and to adopt policies, procedures, and guidelines to manage the state's information resources. The IRMD operates the state's information, telecommunications, voice, video and

data networks as well as the general government data center. 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 including the Statewide Financial Management System (SFMS) and the Oregon State Payroll System (OSPS). The data center also contracts to provide computer services for non-state agencies such as counties and local police departments. Those services

include critical transactions such as queries of the Law Enforcement Data System (LEDS). In addition to the operation of the data center, IRMD provides network support and maintenance through its Network Operations Center (NOC). The NOC maintains the state's wide area network providing connectivity between state agencies as well as public access to information stored on the state's various internet web sites.

INFORMATION SYSTEMS CONTROLS

Information system controls are generally categorized as either general controls or application controls. General controls are intended to protect the environment in which software applications process. Therefore, these controls focus on physical security, data backup and recovery, access controls, operational controls, system development and maintenance, and internal audit. Application controls relate to specific processing requirements of individual software applications. They are designed to reduce the risk of errors in recording, processing, classifying or summarizing of authorized transactions. Application controls ensure that specific software application's data input, processing, and output functions occur as intended.

Application controls interact with, and are complimented by, general controls. General controls coupled with application controls provide additional assurance that authorized transactions processed through the systems are reliable and complete. It is the responsibility of the data center to ensure that its general controls are sufficient to provide an appropriately secure operating environment to protect statewide computer applications.

SCOPE AND METHODOLOGY

Our audit included a review of IRMD's information system general controls relating to the operation of the data center. We performed our field work between January 1998 and July 1998. This work included a review of the control procedures operating during the specified time period for the following control areas:

- Physical security
- Access
- Backup and recovery
- Disaster and contingency planning
- System design, development and maintenance
- Operational procedures
- Organizational responsibilities
- Internal audit
- Network operations

- Year 2000 remediation

The objective of our audit was to evaluate the adequacy of general controls in place at the DAS data center. Our audit work included inquiries of IRMD personnel, examination of documentation supporting controls and procedures, and observation of data center control processes and operations. We evaluated compliance with applicable laws rules and regulations pertaining to internal controls and the operation of the data center. We also reviewed the status of related recommendations contained in our previous audit of the data center, issued in 1995. During our audit we used the Information Systems Audit and Control Foundation's (ISACF) document "Control Objectives for Information and Related Technology" to identify generally accepted and applicable internal control objectives and practices. ISACF is a worldwide organization dedicated to research, develop, and publicize generally accepted information technology control objectives and audit guidelines.

We conducted our audit according to generally accepted government auditing standards. We limited our review to the general controls specified above as they applied to the data center's operations.

AUDIT RESULTS

Access Controls

The Information Resources Management Division (IRMD) has implemented access controls designed to ensure system security. These controls are intended to safeguard information against unauthorized use, disclosure, modification, damage or loss by restricting their access to authorized users. During our review we identified instances where controls could be improved.

The Information Systems Audit and Control Foundation's document "Control Objectives for Information and Related Technology" (COBIT) identifies controls to restrict access to systems, data, and programs to

authorized users. Those controls include, but are not limited to, the following:

- Access to computer resources should be restricted and controlled by mechanisms, such as password protection, to identify and validate users and control their use of the system. Procedures should be in place to keep these mechanisms effective.
- Management should provide access security control based on the individual's demonstrated need to view, add, change or delete data.
- Management should periodically review and confirm access rights.
- Organizations should regularly log, report, review and adjust their security activities to identify and resolve incidents involving unauthorized use of their resources.
- Organizations should periodically evaluate system security to ensure that it performs at its formally approved security level.

The data center relies on a software program called Resource Access Control Facility (RACF) to restrict access to systems, data, and programs. The effectiveness of RACF depends on whether it is properly set-up and maintained, and its output monitored. During our review of the data center's RACF implementation we identified the following areas in need of improvement:

- The data center's RACF administrator assigned conflicting access attributes to data center employees. For example, we found four employees who had both "auditor" and "special" attributes, contrary to RACF specifications, and one employee who possessed powerful "alter" access rights that clearly exceeded her position responsibilities. RACF uses the various levels of access (attributes) to control various security functions within the program.
- Data center management has not reviewed or confirmed access attributes assigned to employees on a routine basis to ensure that they

remain appropriate. Although management informed us that they reviewed access violation reports, during most of our audit period such a review was not documented. Therefore, we could not verify that management reviewed violation reports timely or appropriately resolved possible problems. In response to this concern, data center management has initiated procedures to document their review and any related follow-up action. However, the data center does not have written procedures for reviewing the security violation reports or for resolving exceptions identified by the reports. Those exceptions include routine mistakes as well as incidents involving attempts to gain unauthorized access.

- The data center's RACF implementation does not sufficiently address certain security risks. During our audit we discussed with management those issues that we identified.

The Information Resources Management Division's (IRMD) data center has not established sufficient procedures or managerial oversight to appropriately maintain and monitor its RACF implementation. As a result, the risk that unauthorized transactions may occur or the state's computer resources compromised, has increased.

We recommend that IRMD data center management routinely evaluate the assigned security access rights of its employees and review security incident logs. In addition, we recommend IRMD develop written procedures for timely resolving suspected security problems or incidents. Furthermore, we recommend that IRMD resolve identified RACF security issues and evaluate the adequacy of its current statewide RACF configuration.

Agency Response and Efforts:

IRMD agrees with the audit findings and will take the appropriate steps necessary to implement the recommendation. IRMD has named a

security team, headed by the manager for the General Government Data Center (GGDC), to review this issue so that security problems do not reoccur. This group is responsible for developing security policies and procedures to remedy the following issues:

- *Assignment of RACF attributes, or authorities including documentation of need*
- *Annual review and confirmation of each GGDC employee's RACF authority*
- *Content of RACF reports, establishment of criteria for reviewing RACF reports and recommendations for follow up action*

The security procedures will be completed not later than April 30, 1999. The procedures will include how often records are reviewed, by whom, and processes to be followed if there are errors.

Controls Over Physical Security

IRMD provides physical security controls for the data center intended to protect the equipment and people against man-made and natural hazards. These controls include provisions to limit physical access to the computer center, provisions to ensure that the center's environment is appropriate for operation of the equipment, and controls intended to ensure the safety of those working in the center. IRMD relies on the Department of Administrative Services' Facilities Division to provide and maintain security systems for the data center and the remainder of the building.

IRMD publishes a guideline outlining suggested physical security measures including controls to protect against intrusions. COBIT also describes several "best practices" to ensure that physical security objectives are achieved. COBIT suggests that organizations escort visitors who are in the data center and maintain and review a visitor's log. Furthermore, it suggests that information technology

sites maintain a low profile including limited identification of the site.

During our review we identified weaknesses that, if corrected, could improve physical security at the data center. We found that employees do not always escort data center visitors, nor do they maintain a visitor's log. Further, the data center shares a location with other major technology resources as well as a high profile state agency. Given the high profile of the combined tenants of the site, we concluded that security systems and procedures for the building were inadequate to cover the increased risk.

The above conditions exist because IRMD has not established policies requiring visitor escort or logging of computer center visitors. Furthermore, IRMD in conjunction with DAS's Facilities Division, have not provided sufficient systems or procedures to limit physical access to other vulnerable areas within the building such as the parking structure. Weaknesses in physical security controls increase the risk of unauthorized intrusion and damage to equipment, information and people. Because of the concentration of state technology resources located in and around the data center, the magnitude of damage possible from an incident could significantly impact state computer operations.

We recommend that IRMD design and implement policies requiring visitor escort and visitor logs. In addition, we recommend that IRMD and the Department of Administrative Services' Facilities Division determine appropriate measures for improving physical security of the state's data center. In developing corrective measures, the department should consider costs and benefits of alternative solutions such as improving security at the existing site or moving the data center to a different location.

Agency Response and Efforts:

IRMD agrees with the audit findings. Access to the data center remains a concern of IRMD. Discussions are

underway with Facilities Division to help find additional office space for IRMD staff. Finding additional space will help minimize the number of visitors to the area where the data center is located. Finding alternate office space requires time to implement.

The Facilities Division has dedicated resources to a space needs assessment to be started immediately and concluded in 90 days. Once the assessment is completed, we will have a better idea of options for alleviating IRMD's space needs. The Assistant Division Administrator serves as the space needs coordinator for IRMD.

IRMD will implement policies regarding escorting visitors to the data center and keeping a visitors log. Initiating a visitors log will begin immediately. The manager of the Data Center is responsible for developing a visitor access policy. It will be developed and adopted not later than April 1999.

Internal Audit

The internal audit function is intended to evaluate and monitor the effectiveness of internal controls through cyclical, ongoing reviews. Proactive internal audits provide assurance that intended controls are appropriate and functioning. Effective internal audits also provide valuable feedback to management regarding the achievement of organizational or operational objectives. COBIT indicates that all information technology processes need to be regularly assessed over time for their quality and compliance with control requirements. It also indicates that these functions are enhanced when independent audits are carried out at regular intervals.

Over the past several years the data center operated without an assigned internal auditor specializing in information technology (IT) systems and issues. In addition, during this period other DAS internal audit provided very limited audit coverage of the data center. Thus, the center has

not benefited from independent, regular checks of controls. During our audit, DAS appointed an internal auditor to evaluate information technology systems throughout the agency. DAS's appointment of an IT auditor indicates a significant commitment to provide needed internal audit services.

However, since DAS did not specifically assign the new internal IT auditor to the data center, it is unclear whether the data center's needs will be satisfied.

Lack of independent monitoring increases the risk that intended operational security and other internal controls may be ineffective. In addition, lack of monitoring also increases the risk that internal control errors, inconsistencies, and exceptions may not be systematically documented and reported to management. Furthermore, independent assessments of the center's efforts to achieve organizational objectives may not be performed and communicated to decision makers.

We recommend that the Department of Administrative Services provide increased internal audit coverage to monitor the information technology processes and resources of the data center.

Agency Response and Efforts:

We agree with the recommendation and will focus on providing more audit coverage in the information technology (IT) area. DAS Internal Audit Unit (IA) and the Secretary of State's Audits Division have been working together to coordinate their audit activities to avoid a duplication of effort and conserve state resources. The DAS Internal Audit Committee met with you in early 1998 to discuss ways we could compliment each other's audit coverage. An outcome of that meeting was the decision to rely on the Audit Division's work at the Data Center and to concentrate our audit efforts elsewhere.

All DAS internal auditors are assigned to the Director's Office to ensure independence from operational departments and to ensure access to

senior management. IA provides an independent appraisal function in IT, financial and operational areas. IT audits include reviews of systems under development, data center reviews and application system reviews. IA, comprised of only two auditors, provides this coverage under an annual audit plan. As we develop our 1999 audit plan, we will focus on providing more audit coverage in the IT area, including the data center. The internal audit manager is responsible for the plan's completion in December 1998.

Disaster Recovery and Contingency Planning

Disaster recovery and contingency planning are necessary to ensure that services will be provided in the event of a disruption. COBIT indicates that management should ensure that a written disaster recovery and contingency plan is developed and maintained and that all concerned parties receive regular training on the procedures to be followed. IRMD developed and adopted policy number 03-16 to establish agencies' responsibility for securing, protecting, and recovering information technology resources. That policy indicates that agencies shall develop and maintain contingency plans for their information systems. IRMD's policy states, "the contingency plan will include provisions for physical, data, and personal security; arrangements for use of another system in emergencies when the data are sensitive or mission critical; identify personnel responsibilities and requirements in emergency situations; and be a working document that includes procedures for testing and updating the plan."

Statewide computer systems rely on the state's wide area network (WAN) to connect individual users to the various mainframes and to facilitate interagency e-mail. In addition, the WAN makes it possible for certain non-state entities to interface with state computer systems to transact business or access critical information. IRMD's Network Operations Center is

responsible for developing and maintaining network operations. Thus, it is responsible for ensuring the continuous service of the WAN. During our 1995 audit of IRMD's computer center, we noted that the Network Operations Center lacked a written disaster recovery and contingency plan for restoring critical network information services in the event of a failure. The Network Operations Center has not developed such a plan.

We also reviewed the disaster recovery plan IRMD developed for the mainframe computer system. While a plan was in place, the data center did not perform its remote disaster recovery rehearsal during the current year as suggested by the contractor.

These conditions exist because the Network Operations Center has not devoted sufficient resources or managerial oversight to ensure that disaster recovery plans exist for all critical systems and that training is accomplished. In addition, IRMD indicated that its lengthy negotiations to secure an alternate emergency processing contractor and site made an off-site rehearsal impractical. As a result, the risk is greater that the state may not be able to minimize the effect of a disruption in services in the event of an emergency. Thus, critical systems may be inoperable for an inappropriate period.

We recommend that the Network Operations Center develop and maintain a disaster recovery and contingency plan in accordance with DAS policy number 03-16. This plan should take into consideration relevant items contained in the IRMD's "Disaster Recovery Planning Guideline." In addition, we recommend that IRMD perform on-going and regular disaster recovery training including regular rehearsals.

Agency Response and Efforts:

IRMD agrees with the audit findings. The Network Operations Center in IRMD is developing a Wide Area Network disaster recovery plan. The Network Data Manager is responsible for the plan's completion. It will be completed and implemented not later than December 1998.

The General Government Data Center has a disaster recovery plan contract with Weyerhaeuser Recovery Systems in Federal Way, Washington. IRMD is seeking ISO 9001 Certification. Increasing staff training and scheduling of disaster recovery rehearsals will be part of the ISO 9001 processes outlined for the Data Center. The Data Center manager is responsible for ensuring training and rehearsal schedules are met. Records will be kept documenting staff training and rehearsal schedules.

Year 2000 Compliance

The Department of Administrative Services (DAS) IRMD policy number 03-20 requires that agencies evaluate and test their existing information systems and report their status to the state's Year 2000 coordinator. In addition, agencies are required to certify that their systems satisfy all year 2000 compliance standards.

The data center has appointed an employee to coordinate its year 2000 efforts. The employee is responsible for reporting the center's readiness to the division's year 2000 coordinator. To fulfill this responsibility, he gathers information from custodians of the various system components regarding their anticipated readiness. Our review of the data center's year 2000 project indicates that management has not developed a written comprehensive plan to ensure that all critical data center components will meet year 2000

requirements. In addition, the agency's year 2000 coordinator does not maintain sufficient documentation of the center's remediation efforts to ensure that all necessary aspects will be addressed.

This has occurred because data center management did not provide procedures or oversight to ensure development and documentation of their year 2000 project. Lack of a written comprehensive year 2000 remediation plan may result in the failure of critical state information systems. Because the data center services many other state agencies, this failure could have far-reaching effects.

We recommend that the IRMD provide procedures and oversight to ensure development of a comprehensive, written plan to test and monitor its year 2000 remediation of the data center. This written plan should encompass all aspects of the year 2000 remediation process including inventory, assessment, prioritization, remediation, testing, reliance on third party certification, and contingency planning.

Agency Response and Efforts:

IRMD agrees with the audit findings. A year 2000 testing plan has been developed for the Data Center's mainframe system and third party software. The plan will be fully documented no later than December 1998. The plan includes retaining vendor certification letters and testing of all system and third party software in a mirrored operating environment. A detailed inventory of all mainframe software currently exists, as does a contingency plan. Prioritization and assessment sections of the plan are completed. The Data Center manager is responsible for documenting, updating and implementing the plan.

This report is a public record and is intended for the information of the management of the Department of Administrative Services, the governor of the state of Oregon, the Oregon Legislative Assembly, and all other interested parties. This report 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 Buffinton-Kelm, CPA, CISA* • AUDIT STAFF: *Neal Weatherspoon, CPA; Margaret Kane, CPA*

DEPUTY DIRECTOR: *Sharron Walker, CPA, CFE*

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