Secretary of State

State of Oregon

# DEPARTMENT OF HUMAN RESOURCES

## Computer Center General Controls Review

Audits Division

Secretary of State

State of Oregon

# DEPARTMENT OF HUMAN RESOURCES

## Computer Center General Controls Review

Audits Division

No. 98-49

December 23, 1998

OFFICE OF THE
SECRETARY OF STATE
Phil Keisling
Secretary of State
Suzanne Townsend
Deputy Secretary of State

AUDITS DIVISION
John Lattimer
Director

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

*Auditing for a Better Oregon*

The Honorable John Kitzhaber
Governor of Oregon
State Capitol Building
Salem, Oregon 97310

Gary Weeks, Director
Department of Human Resources
500 Summer Street NE
Salem, Oregon 97310-1012

This report includes our evaluation of the general computer controls in place at the Department of Human Resources Computing Resource Management Data Center. During our audit, we reviewed procedures relating to physical security, access, backup, contingency planning, and other organizational responsibilities. We also reviewed the status of related recommendations contained in our previous audit and evaluated the data center's efforts to ensure year 2000 compliance.

The report includes recommendations to improve access controls, physical security, internal audit coverage, disaster recovery and contingency planning, and processes designed to assure the data center will be year 2000 compliant. The Department of Human Resources agrees with our recommendations.

OREGON AUDITS DIVISION

John N. Lattimer
Director

Fieldwork Completion Date:
August 3, 1998

# TABLE OF CONTENTS

## SUMMARY

### PURPOSE

The purpose of our audit was to evaluate general controls at the Department of Human Resources (DHR) Computing Resource Management (CRM) data center. General Controls are those controls intended to protect the environment in which applications process data. We reviewed control procedures relating to physical security, access, backup, contingency planning, and other organizational responsibilities. We also reviewed the status of prior audit findings and CRM's efforts to ensure that its data center will be year 2000 compliant.

### BACKGROUND

The CRM section operates DHR's data center. The data center processes transactions for all DHR divisions and provides services to the Employment Department. CRM's mainframe is the host for significant DHR payment systems and other software applications supporting critical agency functions.

### RESULTS IN BRIEF

The Computing Resource Management section can improve controls to protect equipment and people, limit physical access, ensure systems security, and provide continuous service.

### RECOMMENDATIONS

Priority Items:

- Improve emergency response procedures.
- Monitor emergency alarms and extinguishing systems.
- Improve physical access systems.
- Improve controls over check stock.
- Develop and implement written procedures to maintain and monitor RACF.
- Develop and maintain a disaster recover and contingency plan.
- Develop a comprehensive year 2000 remediation plan.
- Provide internal audit coverage of the data center.

### AGENCY RESPONSE

The Department of Human Resources agrees with our recommendations.

# INTRODUCTION

The Department of Human Resources (DHR) is Oregon's health and social services agency. The department administers more than 200 programs through six divisions and three program offices. Information systems and services for DHR are provided through the Office of Information Services (OIS). The Computing Resource Management (CRM) section of OIS operates DHR's mainframe data center. CRM's mainframe computer processes transactions for all the divisions within DHR and provides computing services for the Employment Department; therefore, CRM's mainframe is the host for significant DHR payment systems and other software applications supporting critical agency functions. For example, one division processed more than 14 million Medicaid claims totaling $1.3 billion during fiscal year 1995-96, using CRM's mainframe computer system.

CRM is divided into three functional sections including Technical Support, Computer Operations, and Production Services. These sections provide for operation of the mainframe and midrange hardware, related software and consultation services for developing end-user applications.

As are other state data centers, CRM is subject to the Department of Administrative Services Information Resources Management Division (IRMD) policies.

## 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. These controls focus on procedures pertaining to organization and relationships, managing facilities, system security, providing continuous service, resolution of problems and incidents, managing change, managing operations, independent assurance, and compliance with external requirements. Application controls relate to specific processing requirements of individual software applications.

General controls coupled with application controls provide additional assurance that authorized transactions processed through the system are authorized, reliable and complete. CRM is responsible for providing adequate general controls to protect the operating environment of its data center.

## SCOPE AND METHODOLOGY

Our audit included a review of Computing Resource Management's (CRM) information system general controls. We performed our fieldwork between April and August 1998.

The objective of our audit was to evaluate the adequacy of CRM's general controls. Our audit work included inquiries of CRM personnel, examination of documents supporting controls and procedures, and observation of CRM's 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 CRM's data center, issued in 1994. During our audit we used the Information Systems Audit and Control Foundation's (ISACF) document "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 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 controls specified above as they applied to CRM's operations.

# AUDIT RESULTS

## MANAGING FACILITIES

Controls to manage facilities help to protect equipment and people against man-made and natural hazards. The Department of Human Resources Computing Resource Management's (CRM) controls to manage facilities include emergency response procedures, alarms to monitor the computer room environment, fire extinguishing systems, and security systems to limit physical access to the data center. During our review of these controls we found weaknesses that, if corrected, could improve CRM's ability to manage facilities.

We found that CRM's emergency response procedures are incomplete. For example, management has not assigned evacuation coordinators for all shifts and some emergency resources such as the phone tree and employee roster, and procedures are out-of-date. Furthermore, management has not provided on-going emergency response training for employees of the data center.

CRM depends on environmental alarms and fire extinguishing systems to timely detect hazards and to provide protection in the event of an emergency. However, management does not regularly monitor and test those alarms or systems. Furthermore, CRM does not ensure that its outside contractor provides periodic maintenance on the alarms or extinguishing systems as outlined in the service agreement. During our audit, we found a flammable fluid stored in the computer room and noted that one fire exit door was blocked on numerous occasions.

CRM relies on a system of keyed locks and key-card controlled locks to limit physical access to the data center. Although CRM management has informal procedures to monitor this system, they do not always follow those procedures. For example, they do not routinely reconcile the data center's inventory of keys and key-cards. In addition, the operations manager had not revoked key-card access for two employees working job rotations outside of the data center. The manager subsequently revoked the access for one of these employees but has not changed the other. According to the Department of Administrative Services policy, agencies should immediately revoke physical access to computer facilities when employees terminate or are reassigned.

Managing facilities also includes safeguarding assets such as check stock and other negotiable instruments. Because of the financial risk associated with the issuance of checks, the Oregon State Treasury issued policies and procedures requiring state agencies to maintain physical control over check stock. We found that CRM is not meeting the minimum requirements outlined by Treasury including the following:

- Non-authorized employees have access to blank check stock. At our suggestion, CRM management improved this condition by moving the check stock storage key to a more restricted location.

- Management does not conduct and document periodic physical inventories of blank check stock stored at the data center.

- Management has not successfully reconciled check stock nor documented actions to resolve non-reconciling items.

- Employees do not accurately account for check stock usage. For example, we found that the stocking clerk did not record all checks that he received. In addition, check numbers recorded in the inventory log do not always match those received from the manufacturer. For example, the log included entries indicating checks were processed by the data center that the manufacturer reported as excluded from its shipment. Furthermore, CRM’s control logs and other supporting documentation does not include the final disposition of over 400 checks they believed to have been voided. Our investigation indicated that none of those checks were cashed.

CRM has not developed written procedures to evaluate and modify the physical access privileges that it grants to employees. Further, it has not followed established policies and procedures relating to emergency response resources, computer room alarms, and controls over check stock. As a result, CRM may not be able to adequately safeguard its assets or people.

**We recommend** that CRM management make the following improvements to its facility controls:

- Assign an emergency coordinator for all shifts; update emergency resources such as the phone tree and employee roster; provide training to staff on evacuation procedures.
- Monitor alarms and extinguishing systems; ensure its outside contractor provides maintenance for emergency systems as required by the contract agreement; remove unsafe fluids from within the data center; ensure that emergency exits are accessible at all times.
- Develop and implement written procedures to evaluate and modify physical access privileges of CRM employees; periodically perform and document reconciliations of keys and key-cards.
- Comply with the Oregon State Treasury Cash Management Manual's minimum physical controls over check stock.

*AGENCY RESPONSE AND EFFORTS*

*Day shift currently has three Emergency Coordinators (ECs). Both swing and graveyard shifts now have one EC assigned plus an alternate.*

*Policies and procedures dated April 6, 1998 have been given to the shift supervisors to review with employees and ensure they understand the contents.*

*The phone tree and the employee roster are in the process of being updated. Evacuations are planned and scheduled through the Support Services Manager for the Employment Department at 875 Union.*

*Alarms and extinguishing systems are currently monitored during all shifts.*

*Procedures are in place with the appropriate names and numbers of people to be called when an alarm sounds. We currently have a service agreement/contract with Siemens-Cerberus Division to perform routine maintenance and testing on the extinguishing systems inside the center. A procedure has been created to notify the vendor every six months to schedule routine maintenance and testing.*

*Flammable fluids have been removed from the computer center operations area except for necessary alcohol and tape cleaning solvent. Additional tape cleaning solvents are stored at the opposite end of the building in a metal cabinet.*

*Fire exits are clear and will remain clear.*

*At this time a procedure is in place to manually reconcile keys and the key-card system quarterly. This will be accomplished by reviewing and comparing the cardholder file in the security system with a TSO member that is to be updated at the same time the security file is updated. We will also explore a process to automate this reconciliation process.*

*We have requested a copy of the Oregon State Treasury Cash Management manual to enable us to comply with the minimum physical controls over check stock. At the current time we have moved and secured the key to room 9a, where reserve check stock is stored, to a locked area inside the operations area on the 4th floor. Four new logs have been created to record checks being received in room 9a, checks moved from room 9a to the check cage in the operations area on the 4th floor, and checks being removed for usage in production jobs. The fourth log is kept in the report distribution area to log any checks being destroyed. We will also arrange to have an independent person perform a physical inventory and reconcile to the check inventory logs.*

## ENSURING SYSTEM SECURITY

Access controls safeguard information against unauthorized use, disclosure or modification, and damage or loss by restricting its availability to authorized users. The Department of Human Resources (DHR) relies on International Business Machines Corporation’s (IBM) software program Resource Access Control Facility (RACF) to safeguard most programs and data libraries. The effectiveness of RACF depends on whether it is properly set-up, maintained, and its output monitored.

We found the following weaknesses in CRM’s RACF implementation:

- The RACF administrator assigned conflicting access attributes to three employees. These employees had both “special” and “auditor” attributes contrary to RACF’s specifications. RACF’s access attributes control which resources or functions are available to users. According to IBM’s *Auditor’s Guide*, certain RACF access attributes should not be assigned to the same individual to maintain the intended separation of duties.

- Management has not assigned unique user ID’s to employees working in production services, making it difficult to track or monitor their individual activity.

- Management does not ensure that CRM employees change their passwords on a regular basis. Instead, several employees use passwords that they have not changed for years. This has occurred because CRM's RACF administrator allowed the program's automatic password change interval to be turned off for the user ID's. The Department of Administrative Services guideline on system security indicates that each user should change passwords on a regular basis to lessen the risk that passwords will be compromised. In addition, the guideline indicates that information system applications should be programmed to require this regular password change.

- The RACF administrator did not revoke several user ID's in accordance with the Department of Administrative Services guideline on system security. This guideline indicates that user ID's must be revoked if they are not used for 90 days.

- CRM management does not regularly evaluate employee access rights. Further, they do not document review of access violation reports nor any action taken to resolve exceptions identified by the reports. Access violation reports would identify both routine mistakes as well as incidents involving attempts to inappropriately access the system.

The above weaknesses exist because CRM management does not have clear policies and procedures, nor managerial oversight of its RACF implementation. Thus, CRM is less able to protect its systems, data, and programs from unauthorized use, disclosure or modification, and damage or loss.

**We recommend** that CRM management develop clear written policies, procedures, and provide managerial oversight of its RACF implementation. In addition, we recommend that the RACF administrator:

- Set password intervals to automatically require all employees to change passwords every 90 days.

- Revoke all user ID's not utilized within the past 90 days.

- Assign unique ID's to production services staff.

Further, we recommend the technical support manager:

- Review and evaluate the access rights assigned to CRM employees to ensure employees have appropriate access to data and programs.
- Eliminate conflicting RACF attributes.
- Document reviews of security violation reports and any resulting action taken to resolve incidents.

*AGENCY RESPONSE AND EFFORTS*

*CRM management will develop written policies, procedures and managerial oversight of its RACF implementation.*

*Automatically requiring passwords to be changed at regular intervals will be a part of the above policies.*

*Revocation of IDs that have not been used within the past 90 days will be covered in the above procedures.*

*Assigning unique IDs to Production Services staff will be researched and done as long as it can be accomplished without impacting the flow of production through the system.*

*The Technical Support manager and the Operations/Production Services manager will review and evaluate the access rights assigned to their respective employees and make changes as appropriate on an ongoing basis as a part of the above procedures.*

*Conflicting RACF attributes will be researched and dealt with as appropriate.*

*A procedure to review violation reports and record what action was taken to resolve the incidents will be developed.*

## ENSURING CONTINUOUS SERVICE

Disaster recovery and contingency planning are necessary to ensure services will be provided in the event of a disruption. The Department of Administrative Services (DAS) policy 03-16 requires agencies to develop and maintain disaster recovery and contingency plans for their information systems and conduct risk assessments of key information systems. In addition, the policy requires agencies to develop and implement procedures to regularly back-up information system data and store it in a secure off-site location. Back-up procedures should be performed frequently enough to minimize the loss of data that could result in fiscal impacts to the agency or would lower the quality of service that it provides to the public.

Although CRM has a written disaster recovery and contingency plan and procedures for backup and off-site storage of system data, its plan is not current or complete. CRM's management does not conduct periodic tests of disaster recovery and contingency plans or provide on-going disaster recovery training to employees. In addition, CRM has not equipped the off-site storage facility with critical operating manuals and supplies nor updated the emergency briefcases containing minimum software and hardware needed to restore the system and continue operations. Furthermore, CRM's off-site storage facility is located in the basement of a building one block from the data center, contrary to DAS guidelines on physical security. Those guidelines indicate that off-site storage should be located far enough from the facility to not be affected by the same disaster. We also found that CRM management have not conducted risk assessments of key information systems. Risk assessments point out areas of vulnerability or potential losses, and recommends safeguards to reduce those losses.

These conditions exist because CRM management has not provided sufficient managerial oversight or detailed procedures to ensure that disaster recovery and contingency plans are current and complete or to ensure that all significant programs and data are identified, backed up, and moved to the off-site storage facility. Weakness in CRM's disaster recovery and contingency planning decreases its ability to respond to disruptions in service. Thus, critical systems could be inoperable for a longer period in the event of a disaster.

**We recommend** that CRM management make the following improvements:

- Update and complete written disaster recovery and contingency plans.

- Conduct periodic tests or rehearsals of disaster recovery and contingency plans and provide on-going training to employees regarding individual roles and responsibilities.

- Ensure that all critical supplies needed to restore and continue operations are stored at their off-site storage facility.

- Update the emergency briefcases containing minimum software and hardware needed to restore the system.

- Develop and implement detailed procedures to ensure that significant programs and data are identified, backed up, and transferred to its off-site storage facility.

- Conduct a risk assessment of key information systems according to DAS policy.

- Re-evaluate the adequacy and appropriateness of off-site storage facilities to ensure that they meet the DAS guidelines.

*AGENCY RESPONSE AND EFFORTS*

*A 1999/2001 budget request has been made for an additional internal auditor position specifically for information systems audits. A risk assessment of key information systems will be the responsibility of this position.*

*The entire disaster recovery/contingency planning process will be revisited, updated, properly documented and tested. The first step (already in process) will be to get up-to-date system software stored at the disaster recovery site and at the offsite facility.*

## MANAGING CHANGE

CRM is responsible for controlling changes to operating system software and hardware. CRM is also responsible to ensure that its systems will be able to process transactions for the year 2000 and after. However, divisions using the data center are individually responsible for changes to their own application software. According to DAS policy, each agency's responsibility includes evaluating, testing, and certifying that its systems will be year 2000 compliant.

We found that CRM management has not fully determined whether its operating system software and hardware are year 2000 compliant nor assessed the potential impact of non-compliance. In addition, CRM has not determined which system components should be updated or replaced, or identified the earliest time that year 2000 dates will impact each component. Furthermore, CRM has not developed a comprehensive testing plan to certify its systems nor developed contingency plans to be used in the event of a system failure due to non-compliance.

CRM management has not devoted sufficient resources to fully develop and implement a comprehensive written year 2000 remediation plan. Lack of such a plan increases the risk that year 2000 issues will not be corrected, which could result in the failure of critical information systems.

**We recommend** that CRM management develop and implement a comprehensive written year 2000 remediation plan in accordance with the DAS policy.

### *AGENCY RESPONSE AND EFFORTS*

*CRM is in the process of upgrading all system software to be Y2K ready. (In this context, ready means CRM is installing a vendor assured Y2K version of software and developing plans for testing, risk management and contingency as it determines necessary). A comprehensive written plan is being developed. This plan consists of the following: 1) inventory of the software products used on the mainframe, 2) communication with each software vendor to get their Y2K compliant version along with their assurance letter that it is compliant, 3) installation and testing schedule for each product, 4) implementation schedule for all products, 5) hardware inventory and testing plan.*

## MANAGING OPERATIONS

Managing operations includes providing controls to ensure information technology processes occur as intended. To maintain an appropriate operating environment, CRM's management is responsible for ensuring that important operating functions such as authorizing, processing, and recording transactions are separated. This segregation of duties is important to minimize the likelihood of errors or illegal acts occurring and to assure that if such events do occur, they will be detected and corrected timely. To address these issues, DAS provides guidelines on personnel security. Those guidelines indicate that there should be two or more employees on duty at all time. They further state that job rotation should be practiced for individuals in sensitive positions and workflow should be designed to provide as much separation of sensitive functions as possible.

We found that during five hours of CRM's weekend evening shifts the data center is staffed by only two employees. Each of those employees is required to perform both operations and production services functions during the other's break and meal times. Thus, the controls intended to separate functions performed by production services and operations do not exist. For example, the production services employee can initiate programs to print agency checks and at the same time exercise custody over the printed checks. In addition, these employees do not rotate positions, but consistently work the weekend evening shifts.

This condition exists because the Computing Resource Management section does not have policies requiring staff rotation for sensitive positions. In addition, CRM does not have sufficient staffing to ensure that two or more employees are on duty at all times. Inadequate segregation of duties increases the risk that errors or illegal acts could occur and go undetected for an extended period of time.

**We recommend** that CRM management develop and implement policies requiring staff rotation for all sensitive positions. We also recommend that CRM management provide sufficient staffing to ensure appropriate segregation of sensitive duties according to the DAS guidelines on personnel security.

### *AGENCY RESPONSE AND EFFORTS*

*Staff numbers in all sections of CRM have been and continue to be at a level necessary to provide the required service to DHR users. The five hour weekend evening shift issue where two staff performed both operations and production services functions has been addressed and resolved as a result of the reassignment and the re-classing of two positions to shift supervisors. These positions supervise the swing and graveyard shifts in both Operations and Production Services. These positions also rotate every four months. The functions performed during the time an employee is at lunch or on break are minimal. Production Services staff covering for breaks and lunch in Operations only answer the telephones and mount cartridges. When Production Services staff go to lunch or are on breaks they forward the telephone to Operations to be answered during the time they are away from the area.*

*The checks and balances between the scheduling system, the preprocessor and the applications themselves will bring to light any job that is run out of the normal production cycle. With the addition of the shift supervisors on the evening shifts there is more protection from illegal acts and from errors. Cross checking job schedules* *against actual jobs run provides another layer of protection. Also, with the checking done by applications and scheduling dependencies, errors are detected automatically.*

*In addition to the above, CRM will begin to encourage staff as a part of their performance appraisals to take a one to two week vacation at least once a year. This should provide sufficient time to have other employees detect any unusual activities or anomalies.*

## INDEPENDENT ASSURANCE

The internal audit function is intended to evaluate and monitor the effectiveness of internal controls through cyclical, periodic reviews. Effective internal audits can provide assurance that controls are appropriate and functioning. In addition, audits can provide valuable feedback to management regarding the organization's ability to meet operational goals or objectives.

The Department of Human Resources has not provided internal audit coverage of the Computing Resource Management section; thus, CRM has not benefited from independent, regular reviews of practices and procedures.

**We recommend** that the Department of Human Resources provide internal audit coverage to monitor the information technology processes and resources of the Computing Resource Management section.

### *AGENCY RESPONSE AND EFFORTS*

*The DHR internal audit function will provide internal audit coverage for CRM.*

## FOLLOW UP OF PRIOR AUDIT RECOMMENDATIONS

During our current audit we reviewed CRM efforts to implement prior audit recommendations.  Our prior audit report No. 94-04 included 26 audit recommendations.  Of those recommendations, CRM has fully resolved seven. We addressed the remaining unresolved or partially resolved issues within the context of our current audit recommendations.

## REPORT DISTRIBUTION

This report is a public record and is intended for the management of the Department of Human Resources, the governor of the state of Oregon, the Oregon Legislative Assembly, and all other interested parties.

## COMMENDATION

The courtesies and cooperation extended by the officials and staff of the Department of Human Resources during the course of this review were commendable and sincerely appreciated.

## AUDIT TEAM

Nancy Buffinton-Kelm, Audit Administrator, CPA, CISA
Neal Weatherspoon, CPA
Nancy L. Young, CPA
Shandi C. Maxwell

# FACTS ABOUT THE SECRETARY OF STATE AUDITS DIVISION

The mission of the Audits Division is to "Protect the Public Interest and Improve Oregon Government." The Oregon Constitution provides that the Secretary of State shall be, by virtue of his office, Auditor of Public Accounts. The Audits Division exists to carry out this duty. The division reports to the elected Secretary of State and is independent of the Executive, Legislative, and Judicial branches of Oregon government. The division audits all state officers, agencies, boards, and commissions and oversees audits and financial reporting for local governments.

DIRECTORY OF KEY OFFICIALS

| | |
|---|---|
| *Director* | John N. Lattimer |
| *Deputy Director* | Catherine E. Pollino, CGFM |
| *Deputy Director* | Sharron E. Walker, CPA, CFE |

This report is intended to promote
the best possible management of public resources.

If you received a copy of an audit and no longer need it, you may return it to the Audits Division. We maintain an inventory of past audit reports. Your cooperation will help us save on printing costs.

Oregon Audits Division
Public Service Building
Salem, Oregon 97310

503-986-2255

We invite comments on our reports
through our Hotline or Internet address.

Hotline: 800-336-8218
Internet: Audits.Hotline@state.or.us
http://www.sos.state.or.us/audits/audithp.htm

***Auditing to Protect the Public Interest and Improve Oregon Government***