



Charles A. Hibner, Director, Audits Division

Bill Bradbury, Secretary of State

# Secretary of State Audit Report

## Oregon Department of Administrative Services: Statewide Financial Management Application Computer Controls Review

### Summary

#### BACKGROUND

The Department of Administrative Services (department) provides centralized services to state agencies, including maintenance of computer networks and operation of the State Data Center.

The department's State Controller's Division provides centralized accounting and reporting services and is responsible for operation and control of the Statewide Financial Management Application (SFMA).

Most state agencies use the Relational Statewide Accounting and Reporting System (R\*STARS), a sub-system within SFMA, as their primary general accounting application. State agencies also rely on R\*STARS data contained in the state Data Mart for ad hoc reporting. In addition, the department uses R\*STARS data to prepare the Comprehensive Annual Financial Report (CAFR) for the State of Oregon. The SFMA and Data Mart are currently hosted at the department's State Data Center.

The purpose of this audit was to evaluate the effectiveness of selected general and application computer controls governing the department's R\*STARS implementation. This is an annual audit performed in support of our audit of the state's CAFR. Specific audit objectives were to evaluate controls governing data integrity, program modifications, backup and restoration processes, and system security.

#### RESULTS IN BRIEF

Based on our audit work, we found that:

- Application controls provided reasonable assurance that system data input by agencies' staff would remain complete, accurate and valid. Those controls also reasonably assured that the Data Mart would accurately represent information contained in R\*STARS transaction files.
- Department procedures ensured that system modification requests were appropriately

prioritized, authorized, assigned, documented, tracked and tested.

- System managers did not have assurance that backup tapes were viable or were stored off-site. In addition, the department did not have adequate procedures for restoring the system in the event of a disaster or major disruption.
- Logical access controls provided a vital layer of security to reasonably protect the system. However, the system was at increased risk of compromise due to security weaknesses at the State Data Center.

#### RECOMMENDATIONS

We recommend:

- The State Controllers Division and State Data Center management develop a written service level agreement to clarify responsibilities and expectations for backup and disaster recovery services, including assurance that backup tapes are viable and stored as directed.
- The department develop and test comprehensive disaster recovery procedures to ensure timely restoration of R\*STARS in the event of a major disruption. Those procedures should fully document the various recovery roles, responsibilities and expectations, including services that will be provided by the State Data Center.
- The department ensure the recommendations we included in the State Data Center confidential security report are timely implemented.

#### AGENCY'S RESPONSE

*The Department of Administrative Services generally agrees with the recommendations.*

## Background

The Department of Administrative Services (department) provides centralized services to state agencies such as payroll, purchasing, printing, motor pool, and facilities management.

The department's State Controller's Division provides statewide accounting and reporting services and is responsible for operation and control of the Statewide Financial Management Application (SFMA).

SFMA was developed by KPMG Peat Marwick and implemented by the department in the 1990's. It is comprised of two sub-systems, the Relational Statewide Accounting and Reporting System (R\*STARS) and the Advanced Purchasing and Inventory Control System (ADPICS). Most state agencies use R\*STARS as their primary general accounting system.

To enable more robust reporting, selected current and historical R\*STARS information is also stored on the department's Data Mart. The department uses R\*STARS and Data Mart information to prepare the state's Comprehensive Annual Financial Report (CAFR).

The SFMA and Data Mart are currently hosted at the department's State Data Center. Modifications to SFMA programming code are performed by members of the department's Operations Division – Enterprise Application Services.

## Purpose

The purpose of this audit was to evaluate the effectiveness of key general and application computer controls governing the R\*STARS portion of the department's Statewide Financial Management Application.

This is an annual audit performed in support of our audit of the state's

Comprehensive Annual Financial Report.

General controls are embedded in information technology processes. They are designed to protect the environment in which all software applications operate. Examples of general controls include system development methodologies, program change management procedures, security, and backup routines.

Application controls are embedded in business processes. They are application specific controls designed to enforce internal controls or ensure system information remains complete, accurate and valid.

## Audit Results

### Application Controls Reasonably Ensured R\*STARS Data Integrity

Effective application controls include both manual and automated processes to ensure only complete, accurate, and valid information is entered into a computer system; data integrity is maintained during processing; and system outputs conform to anticipated results.

We found that manual and automated application controls governing R\*STARS were well documented. In addition, the department had detailed written procedures to guide staff and system users regarding control processes.

To verify that controls were working as intended, we performed various tests of key application controls. Specifically, we evaluated controls governing:

- system profile change management,
- error detection and correction,
- audit trails,

- accounting cycle closing processes, and
- transfer of information to the Data Mart.

In addition, we tested application data to ensure they included necessary elements and conformed to established formats. We also tested Data Mart files to determine whether they matched information recorded in R\*STARS.

Based on the results of these tests, we concluded that application controls provided reasonable assurance that system data input by agencies would remain complete, accurate and valid. We also concluded that controls provided reasonable assurance that the Data Mart would accurately represent information contained in R\*STARS transaction files.

### The Department Followed Appropriate System Development Processes and Change Management Procedures

Management should ensure that all changes to computer applications are appropriately authorized, documented, tested and approved. Proper change management processes should also ensure that only approved program modifications are implemented.

Employees of the Statewide Financial Management Services (SFMS) section of the State Controller's Division were responsible for approving, testing, and implementing R\*STARS program modifications. The department's Enterprise Application Services (EAS) staff were assigned to make programming code changes as directed by SFMS managers.

We evaluated the department's system development and program change management procedures for R\*STARS. Based on those tests,

we concluded that the department's procedures were sufficient and effective to ensure system modification requests were appropriately prioritized, authorized, assigned, documented, tracked and tested by EAS and SFMS staff.

### **Backup and Disaster Recovery Strategies were Incomplete**

Organizations should ensure that usable backups are regularly performed in accordance with a defined back-up strategy. This strategy should ensure all critical files are copied as frequently as needed to meet business requirements. System disaster recovery procedures should also be well documented and tested to ensure proper and timely restoration of the system in the event of a major disruption.

Department staff ensured weekly backup tapes of critical R\*STARS files were created at the State Data Center. However, they did not have assurance that backup tapes were viable or were stored off-site. The department also did not have adequate procedures for restoring the system in the event of a major disruption. In addition, it did not have a written service level agreement with the State Data Center to clarify disaster recovery roles, responsibilities, and requirements. As a result, timely or successful restoration of the system in the event of a major disruption would likely be problematic.

These findings are similar to those we had in our prior audit of the system (report 2007-31). In response to that audit, department management indicated they were actively involved in developing a solution to the findings. However, our current work shows that those efforts were not sufficient to ensure adequate backup and recovery.

**We recommend** that State Controllers Division and State Data Center management develop a written service level agreement to clarify each division's responsibilities and expectations for backup and disaster recovery services. That agreement should include assurance that backup tapes are viable and stored as directed.

#### ***Agency's Response:***

*On July 28, 2008 the SDC Advisory Board approved a written service catalog. This service catalog included defined roles and responsibilities that were agreed upon by SDC and agency participants. The sections of the service catalog that address these specific concerns are 1. SDC Storage Services, 2. Storage and Space Management 3. Backup, Restore, and Recovery and 4. Continuity and Recovery Management.*

*The department, as a customer of the data center, will develop a service level agreement relating to the services the data center provides (as outlined by the service catalog). This SLA will outline appropriate protocols for the various program/division application and services that reside at the data center so expectations are defined and followed.*

**We also recommend** that the department develop and test comprehensive disaster recovery procedures to ensure timely restoration of R\*STARS in the event of a major disruption. Those procedures should fully document the various recovery roles, responsibilities and expectations, including services that will be provided by the State Data Center.

#### ***Agency's Response:***

*We agree with this recommendation. SDC has outlined internal procedures for disaster recovery. Enterprise Application Services (EAS) and SDC have also indicated they have disaster*

*recovery procedures. The procedures and processes have not been tested and SCD will work with EAS and SDC to perform testing of the defined procedures.*

### **Logical Access Controls Were Adequate But Data Center Weaknesses Pose Risks**

Executive management is responsible for establishing an overall approach to security and internal control that ensures the integrity of computer systems and other information assets. Effective security should follow a layered approach that protects the environment in which systems operate and logical access controls to ensure system assets are further protected against unauthorized use, disclosure, modification, damage or loss.

Logical access to computer applications should be restricted according to each user's individual need to view, add or alter information. In order to maintain this principle of "least-privilege," organizations should have formal processes for timely granting, issuing, suspending and closing user accounts. In addition, management should periodically review and confirm users' access rights to ensure they remain appropriate.

Logical access to R\*STARS screens was primarily controlled through program code that limited access to data and resources based on information stored in user account profiles.

We evaluated the department's processes for granting and managing user account profiles. In addition, we tested user profiles to determine whether they conformed to the department's internal control policies. Furthermore, we reviewed other logical access mechanisms that protected system files and data

from access not initiated through the application.

We found that these controls were operating as intended and provided a vital layer of security to protect the system against unauthorized use, disclosure, modification, damage or loss. However, on August 6, 2008, we issued a separate confidential audit report (2008-CS1) to communicate the results of security work we performed during a separate audit of the State Data Center, which hosts the R\*STARS system. Within that report, we identified specific security weaknesses relating to the computing environment provided by the data center.

Based on these results, we concluded that the system and its data were reasonably protected against unauthorized use, disclosure, modification, damage or loss. However, the system was at increased risk of compromise due to security weaknesses at the State Data Center.

We recommend that the department ensure the recommendations we included in the State Data Center confidential security report are timely implemented.

**Agency's Response:**

*As stated in our response to your State Data Center confidential security report No. 2008-CS1 dated August 6, 2008, management believes security may be further enhanced through careful considerations of the review's findings and recommendations. We will continue to work toward progress on these issues as specifically addressed in that document.*

**Audit Objectives, Scope and Methodology**

Our audit objective was to evaluate the effectiveness of key

general and application computer controls governing the R\*STARS portion of the department's Statewide Financial Management Application. Specifically, we determined whether the department implemented controls to provide reasonable assurance that:

- R\*STARS data would remain complete, accurate and valid during system input, processing and output;
- R\*STARS program modifications followed approved system development processes and change management procedures;
- R\*STARS could be timely restored in the event of a major disruption; and
- R\*STARS data was protected against unauthorized use, disclosure, modification, damage or loss.

To achieve these objectives, we interviewed various department personnel, examined system documentation, and used standard query tools to analyze electronic data.

To test application controls, we evaluated profile change management processes, error detection and correction routines, audit trails, accounting cycle closing processes, cost allocation processes, and Data Mart load procedures. In addition, we performed various electronic integrity tests of March 2008 R\*STARS and Data Mart data.

We tested program change management controls by evaluating related policies and procedures, system file metadata, and documentation relating to selected program modifications.

For backup and recovery objectives, we reviewed the process for creating backups, and evaluated the department's backup and recovery procedures and plans.

To determine whether the application and its data were reasonably secure, we reviewed and evaluated department security policies and procedures, logical access to system files, and logical access controls provided through R\*STARS.

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.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.



**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: *Neal E. Weatherspoon, CPA, CISA, CISSP*

AUDIT STAFF: *Mark A. Winter, CPA, CISA  
Sarah A. Anderson  
Jason A. Butler*

DEPUTY STATE AUDITOR: *William K. Garber, CGFM, MPA*

*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/index.html>*

*by phone at 503-986-2255*

*or by mail from:*

*Oregon Audits Division  
255 Capitol Street NE, Suite 500  
Salem, OR 97310*