



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

Summary

Charles A. Hibner, Director, Audits Division

Bill Bradbury, Secretary of State

Secretary of State Audit Report

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. In addition, the department uses R*STARS data to prepare the Comprehensive Annual Financial Report (CAFR) for the State of Oregon.

The purpose of this audit was to evaluate the effectiveness of key general and application computer controls governing the department's R*STARS implementation. Specific audit objectives were to evaluate controls governing data integrity, program modifications, system security, and backup and restoration processes.

RESULTS IN BRIEF

Based on our audit work, we found that:

- Application controls provided reasonable assurance that R*STARS data would remain complete, accurate and valid.
- Final technical reviews of program modifications and their subsequent elevation to production were performed by the programming group who made the changes. Thus, department managers did not have full assurance that only appropriate changes were made.
- Backup tapes of critical SFMA files were created at the State Data Center on a regular basis, but those tapes were not periodically tested for usability.

- Timely restoration of SFMA in the event of a major disruption could be problematic because the department did not have a defined and tested recovery plan.
- Logical access controls provided reasonable assurance that system files and data were protected against unauthorized use, disclosure, modification, damage or loss.

RECOMMENDATIONS

We recommend that department management:

- Require independent technical reviews of code modifications prior to approval and elevation to production, and further limit logical access to approved code to provide more positive assurance that only approved code will be moved to production.
- Develop, implement and test strategies to ensure recovery roles and responsibilities are defined, assigned and formally coordinated with the State Data Center via a written service level agreement.
- Coordinate with the State Data Center to ensure backup tapes are periodically tested to ensure their usability.

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.

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.

During our audit, 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 data 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 would remain complete, accurate and valid as input by agencies. We also concluded that controls provided reasonable assurance that the Data Mart would accurately represent information contained in R*STARS transaction files.

Final Review of Program Modifications Should Be Improved

Management should ensure that 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 managing SFMA, including approving, testing and implementing SFMA program modifications. The department's Enterprise Application Services (EAS) staff, who work within the Operations Division, were assigned to make programming code changes as directed.

We evaluated the department's system development and program change management procedures for SFMA. 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 SFMS staff.

We noted, however, that the same few EAS staff who made SFMA programming changes performed the final technical review of the code to ensure only approved changes were made. In addition, those same individuals subsequently had full access to the approved code and were assigned to move the code into production.

Because the above duties were not adequately separated, department managers did not have full assurance that all program modifications contained only authorized and approved changes. The EAS manager responsible for SFMA programming indicated that this condition was the result of the limited number of technically qualified staff available to perform these duties.

We recommend that department management require independent technical reviews of code modifications prior to approval and elevation to production. We also recommend that the department further limit logical access to approved code to provide more positive assurance that only approved code will be moved to production.

Agency's Response:

We agree that implementing this recommendation would be ideal. However, current staffing levels do not provide the expertise necessary to perform independent technical reviews of code prior to elevation into production. We are currently exploring options that would allow us to implement this recommendation. Options include software packages designed to monitor and track these types of code changes and working with other state agencies who have similar needs. The Operations Division staff will work closely with the State Controller's Division (SCD) staff to research available options and determine the costs and benefits of each prior to implementing any changes.

Disaster Recovery Strategies Were Inadequate

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. In addition, restoration procedures should be well documented to facilitate proper and timely recovery of files in the event of a major disruption.

The department ensured that backup tapes of critical SFMA files were created at the State Data Center on a regular basis. However, the department had not ensured that backup media was regularly tested by data center staff to ensure its usability.

More importantly, the department had not defined in written procedure, or formal service level agreement with the State Data Center, how the system would be restored should a major disruption of services occur.

Based on the above, we concluded that timely or successful restoration of the system in the event of a major disruption would likely be problematic.

We recommend that department management coordinate with the State Data Center to develop, implement, and test strategies to ensure timely restoration of the system in the event of a major disruption of system services. Those strategies should fully document the various recovery roles, responsibilities and expectations of all parties involved in a recovery effort. The above should also be appropriately annotated within a formal service level agreement with the State Data Center.

Agency's Response:

We agree with the recommendation and are actively engaged in developing a plan.

We also recommend that the department coordinate with the State Data Center to ensure backup tapes are periodically tested to ensure their usability.

Agency's Response:

We also agree that the State Data Center (SDC) backup tapes should be tested. At this time, a method to test the backup tapes in a test environment has not been identified. Testing backup tapes in production would mean agency keyed transactions would need to be re-keyed for one entire day. SCD will continue to work with the Operations Division and the SDC to find a non-production method and environment to test the process. After the process has been identified, we are committed to periodically testing to ensure the usability of backup tapes.

Logical Access Controls Reasonably Protected the System

Executive management is responsible for establishing an overall approach to security and internal control that is sufficient to maintain integrity of computer systems and protect resources. In that regard, effective logical access controls provide a vital layer of protection to prevent 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 that they remain appropriate.

Logical access to SFMA 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 direct access not initiated through program control.

Based on the results of this work, we concluded that logical access controls provided reasonable assurance that system files and data were protected against unauthorized use, disclosure, modification, damage or loss.

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;
- program modifications followed approved system development processes and change management procedures;
- the system could be timely restored in the event of a major disruption; and
- the system 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 May 2007 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 verified the existence of backup media, 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 SFMA.

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

AUDIT STAFF: *Diane Farris, CPA
Erika A. Ungern, CISA
Mary Doel
Michelle Searfus*

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*