



Secretary of State Audit Report

Statewide Financial Management Application: Accounting System Continues to be Reliable, but Security and Disaster Recovery Risks Remain

Summary

BACKGROUND

The Department of Administrative Services (department) provides centralized services to state agencies including operation and control of the Statewide Financial Management Application (SFMA) and its Relational Statewide Accounting and Reporting System (system).

Most state agencies use the system as their primary general accounting application and as the basis for statewide financial reporting. They also rely on system data contained in the department's Datamart for ad hoc reporting.

The purpose of this audit was to evaluate the effectiveness of selected general and application computer controls governing the system. Our 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:

- State agencies can rely on the system to accurately process financial transactions and maintain accounting records. They can also rely on the Datamart to accurately reflect detailed accounting transactions processed by the system.
- The department appropriately controlled changes to system code by ensuring only authorized changes could be made. These controls were critical to ensure unauthorized program modifications could not be used to render application controls ineffective, or otherwise jeopardize the integrity of the system and its data.
- Restoration of the system following a major disruption would likely be problematic because the department did not test its restoration plans and relied on unproven State Data Center capabilities.

In addition, the department did not ensure backup tapes were viable or were transferred off-site as directed.

- State Data Center weaknesses pose significant security risks because they render logical access controls significantly less effective. Because of the sensitive nature of security, we communicated these issues to the department in a confidential management letter prepared in accordance with ORS 192.501 (23), which exempts such information from public disclosure.

RECOMMENDATIONS

We recommend that department management:

- ensure system disaster recovery tests are conducted to validate and further refine recovery strategies; ensure the State Data Center has the proven capability to timely restore enterprise infrastructure and coordinate enterprise recovery efforts; obtain assurance that system backup tapes are viable and stored off-site; and
- ensure the recommendations included in our confidential management letter are timely implemented.

AGENCY'S RESPONSE

The Department of Administrative Services generally agrees with the recommendations. The department's response is attached to this report, beginning on page 5.

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).

The department implemented the SFMA in the mid 1990's. The accounting subsystem within SFMA is the Relational Statewide Accounting and Reporting System (system). Most state agencies use the system as their primary general accounting application.

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

The SFMA and Datamart are currently hosted at the department's State Data Center. Modifications to system 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 system. We perform this audit annually to provide internal control information needed for subsequent financial audits, including our audit of the CAFR, and to provide agency management a basis to evaluate overall risk.

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.

Our specific audit objectives were to evaluate controls governing data integrity, program modifications, backup and restoration processes, and system security.

Audit Results

Agencies Can Rely on the System to Accurately Process and Maintain Accounting Records

We concluded that state agencies can rely on the system to accurately process financial transactions and maintain accounting records. They can also rely on the Datamart to accurately reflect the detailed accounting transactions processed by the system.

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 noted the department provided a variety of manual and automated controls to ensure the system processed transactions correctly and outputs occurred as intended. Some of these controls included:

- automated routines to ensure transactions are posted

according to predefined accounting structures;

- centrally maintained profiles to ensure agencies post transactions to approved budgets;
- automated routines that ensure transactions are posted to valid cash accounts;
- system edits to ensure individual data elements are complete and appropriately formatted prior to processing;
- control reports to enable account balancing and facilitate timely error detection and correction;
- Datamart file load routines that ensure congruency with system information; and
- procedures to ensure accounting cycles are closed appropriately.

We verified that these controls were functioning to ensure system data would remain complete, accurate and valid during input, processing and output. We also confirmed that the Datamart was an accurate repository of system transactions.

The Department Appropriately Controlled Changes to System Code

Our test results indicated that key system development and change management controls were functioning as intended and provided reasonable assurance that only authorized changes were made to system code. This is critical because unauthorized program modifications could be used to render application controls ineffective, or otherwise jeopardize the integrity of the system and its data.

Managing changes to information systems minimizes the likelihood of disruption, unauthorized alterations, and errors. Effective system development and change

management controls do this by ensuring that program changes are appropriately authorized, documented, tested, and approved.

During our audit we tested the department's processes for:

- initiating, approving, and prioritizing proposed system changes to ensure they are authorized by system owners and meet business needs;
- testing and approving modified code to ensure it satisfies requirements included in requests;
- documenting system changes to ensure they are clearly linked to change requests, approvals, testing, and elevation to production; and
- performing independent technical reviews of code, including automated code compares to ensure only authorized changes are made.

We found that these controls were operating to ensure system modifications were appropriately requested, prioritized, authorized, assigned, documented, and tracked by department staff.

Restoration of the System Following a Major Disruption Would Likely Be Problematic

Restoration of the system following a major disruption would likely be problematic because the department did not test its restoration plans and relied on unproven State Data Center capabilities. In addition, the department did not ensure backup tapes were viable or were transferred off-site as directed.

Organizations should ensure 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.

We found that department staff verified that daily and weekly backup tapes of critical system files were created at the State Data Center. However, State Controller's Division management had not confirmed that State Data Center staff tested backup tapes for viability or transferred them off-site as directed.

We also noted that Enterprise Application Services staff had developed automated procedures to recover system files and data, but had not tested these procedures. Moreover, recovery plans were contingent on the State Data Center's ability to timely restore enterprise infrastructure and to coordinate an enterprise recovery effort. Our inquiries revealed that these critical State Data Center capabilities had not yet been developed or tested.

We recommend that the department ensure system disaster recovery tests are conducted to validate and further refine recovery strategies, and ensure the State Data Center has the proven capability to timely restore enterprise infrastructure and coordinate enterprise recovery efforts.

We also recommend that State Controller's Division management obtain assurance that system backup tapes are viable and stored off-site.

Agency's Response:

The department's response is attached to this report, beginning on page 5.

State Data Center Weaknesses Pose Significant Security Risks

We found that logical access controls were well managed and provided a vital layer of protection. However, the system is at risk because of specific security weaknesses in controls provided by the State Data Center.

Effective security should follow a layered approach that protects the environment in which systems operate and includes logical access controls to ensure system assets are further protected against unauthorized use, disclosure, modification, damage, or loss.

Two divisions within the department are responsible for providing security for the system. The State Controller's Division is responsible for maintaining logical access profiles. The State Data Center is responsible for securing the computing environment, including operating system platforms, data storage, and networks.

During our evaluation of system security, we found that the department had effective controls for granting and managing user accounts and for ensuring that user profiles conformed to internal control policies. In addition, logical access mechanisms were designed to protect system files and data from access not initiated through the application. However, we noted that specific State Data Center security weaknesses rendered these logical access controls significantly less effective. As a result, the system and data were not reasonably protected.

Because of the sensitive nature of security, we communicated these issues to the department in a confidential management letter outlining specific details of our findings and recommendations to improve security. We prepared that letter in accordance with

ORS 192.501 (23), which exempts such information from public disclosure.

We recommend that the department ensure the recommendations included in our confidential management letter are timely implemented.

Agency's Response:

The department's response is attached to this report, beginning on page 5.

Audit Objectives, Scope and Methodology

Our audit objectives were to determine whether controls governing the Relational Statewide Accounting and Reporting System (system) provided reasonable assurance that:

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

During our audit, we interviewed various department personnel, examined system documentation, and used standard query tools to analyze electronic data.

Specifically, to verify application controls were working as intended, we:

- tested a selection of centrally maintained profiles to ensure changes were properly approved and documented;
- tested a selection of user security access requests for

appropriate authorization and segregation of duties;

- examined selected control reports for evidence of review and follow-up;
- tested a selection of data files from October and November 2008 to ensure all necessary elements were included and data conformed to established formats;
- reviewed procedures for uploading data to the Datamart;
- compared Datamart files to corresponding system information;
- reviewed a selection of cost allocation runs to ensure controls for preventing overspending of budgetary allocations were functioning; and
- reviewed accounting cycle closing documentation to ensure year end processes were properly controlled.

To test program change management controls, we examined related policies and procedures, system file metadata, and documentation relating to selected program modifications.

To evaluate backup and recovery controls, we reviewed processes for creating backups, and evaluated the department's backup and recovery procedures and plans.

To address security objectives, we:

- evaluated processes for granting and managing user accounts;
- determined whether user profiles conformed to the department's internal control policies;
- tested other logical access mechanisms designed to protect system files and data from access not initiated through the application; and

- inquired whether prior State Data Center security weaknesses had been resolved.

We used the IT Governance Institute's 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 we obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.



Oregon

Theodore R. Kulongoski, Governor

Department of Administrative Services

Office of the Director
155 Cottage Street NE, U20
Salem, OR 97301-3966
(503) 378-3104
FAX (503) 373-7643

April 22, 2009

Neal E. Weatherspoon, CPA, CISA, CISSP
Audit Manager, Audits Division
Office of the Secretary of State
255 Capitol Street NE, Suite 500
Salem, OR 97310

Re: Statewide Financial Management Application Computer Controls Review

Dear Mr. Weatherspoon:

Thank you for providing us the draft report regarding the Statewide Financial Management Application (SFMA) on April 13, 2009. We appreciate the time and effort your team has spent reviewing this program over the last three months. The Department of Administrative Services (Department) generally agrees with the recommendations as stated in the report and offers the following specific responses to the two areas noted for improvement:

The report recommended: **Department management ensure system disaster recovery tests are conducted to validate and further refine recovery strategies; ensure the State Data Center has the proven capability to timely restore enterprise infrastructure and coordinate enterprise recovery efforts; and obtain assurance that system back-up tapes are viable and stored off-site.**

Internally, the SDC has conducted a detailed analysis of deficiencies for DR and has appointed a DR project manager, a DR solutions team, and primary and secondary DR coordinators representing each SDC domain. The project team is establishing and implementing a formal plan, analyzing software tools to create application infrastructure inventories and maps, and establishing new tools and processes to better record, report, and recover new application configurations.

Externally, the SDC meets regularly with external (agency) DR coordinators who are identifying critical applications, recovery time objectives, and recovery point objectives. The SDC is also working with agency DR coordinators to establish recovery options for the agencies critical applications.

In December of 2008 the SDC completed the establishment of a statewide contract with an external vendor for Disaster Recovery services. Services provided by the external vendor are available for procurement by all state agencies through this price agreement include DR recovery, testing and consulting. Investing in the development and maintenance of fully operational DR planning, testing and recovery has been an ongoing issue for state agencies. The financial aspects of this issue have been escalated to the state's finance committee. The recommendations from the finance committee are and will be approved through Agency Directors.



Page 2
April 22, 2009
Neal Weatherspoon, CPA, CISA, CISSP
Office of the Secretary of State

We agree with the recommendations and are actively working with the State Data Center to put into place a process that will provide assurances that system back-up tapes are stored off-site, and are committed to putting into place procedures that will ensure the viability of the off-site tapes.

The report recommended: Department management ensure the recommendations included in our confidential management letter are timely implemented.

We are responding under separate cover.

The Department appreciates the audit team's help in analyzing the controls over SFMA. If you have any further questions, please contact Joy Sebastian, Deputy State Controller, at (503) 373-1044, extension 228 or Joy.Sebastian@state.or.us.

Sincerely,



Kris Kautz, Deputy Director
Department of Administrative Services

cc: Scott Harra, DAS Director
Drummond Kahn, Oregon Audits Division Interim Director
John Radford, DAS Administrator, State Controller's Division, DAS
Joy Sebastian, Deputy State Controller, DAS
Pamela J. Stroebel Valencia, DAS Chief Audit Executive



**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
David Terry, CPA
Nicole Rollins*

DEPUTY DIRECTOR: *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*