

---

Secretary of State

State of Oregon

**DEPARTMENT OF ADMINISTRATIVE SERVICES**  
**Statewide Financial Management System (SFMS)**  
**Computer Application Controls**



Audits Division

---



---

Secretary of State

State of Oregon

**DEPARTMENT OF ADMINISTRATIVE SERVICES**  
**Statewide Financial Management System (SFMS)**  
**Computer Application Controls**



**Audits Division**

---



OFFICE OF THE  
SECRETARY OF STATE  
Bill Bradbury  
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, M.D.  
Governor of Oregon  
State Capitol Building  
Salem, Oregon 97310

Jon Yunker, Director  
Department of Administrative Services  
155 Cottage Street NE  
Salem, Oregon 97310

This report includes our evaluation of selected computer controls governing the Department of Administrative Services (DAS) Statewide Management Information System (SFMS) and its related Data Mart. During this audit, we evaluated controls to limit access to these systems and procedures to ensure that information included in the Data Mart accurately reflect corresponding SFMS transactions. We also reviewed the status of related recommendations contained in our previous audits relating to SFMS operations.

This report includes recommendations to improve SFMS and Data Mart controls. The Department of Administrative Services generally agrees with our recommendations.

OREGON AUDITS DIVISION

John N. Lattimer  
Director

Fieldwork Completion Date:  
April 8, 1999



# TABLE OF CONTENTS

	<u>Page</u>
SUMMARY .....	vii
INTRODUCTION	
INFORMATION SYSTEMS CONTROLS.....	1
SCOPE AND METHODOLOGY .....	1
AUDIT RESULTS	
ACCESS CONTROLS.....	3
DATA MART OPERATIONS AND MAINTENANCE .....	5
STATUS OF PRIOR AUDIT FINDINGS.....	6
COMMENDATION .....	7
APPENDIX A .....	9
AGENCY’S RESPONSE TO THE AUDIT REPORT .....	11



## SUMMARY

### BACKGROUND

SFMS is the state's centralized accounting and purchasing system. The Department of Administrative Services (DAS), State Controller's Division (SCD) administers SFMS and is responsible for providing internal controls to protect the system. SFMS processes financial transactions and provides financial information for most state agencies. Furthermore, SCD uses SFMS data to produce the state's comprehensive annual financial report.

In April 1997, SCD implemented its Accounting Data Mart (data mart). The data mart is an ad hoc reporting facility containing weekly updates of selected SFMS data. The data mart permits agencies to generate customized reports to facilitate their decision-making. After two years of operation, the data mart contains approximately 60 million records representing over \$2.5 trillion in transactions. SCD works in cooperation with the DAS General Government Data Center to control access to the data mart.

### AUDIT PURPOSE

The purpose of our audit was to evaluate selected computer application controls for SFMS. Application controls are designed to reduce the risk of unauthorized, inaccurate, or incomplete input, processing, output, and storage of transactions for a specific application.

### AUDIT RESULTS

The Department of Administrative Services should consider the following priority items to improve its control over SFMS and the Data Mart:

- Improve procedures for maintaining and monitoring SFMS access controls.
- Establish effective methods for granting and maintaining non-standard user access privileges.
- Conduct more thorough semi-annual reviews of user access privileges and ensure agency security officers understand and perform their responsibilities regarding those reviews.
- Develop written policies and procedures for Data Mart operations, security, and data integrity.
- Fully resolve all outstanding prior audit findings.

**AGENCY'S RESPONSE** The Department of Administrative Services generally agrees with our recommendations. The department's full response can be found on page 11 of this report.

## **INTRODUCTION**

The Statewide Financial Management System (SFMS) is the state's centralized accounting and purchasing system. The Department of Administrative Services (DAS), State Controller's Division (SCD) is responsible for administering SFMS. In addition, SCD is responsible for providing internal controls to protect the system from unauthorized or inappropriate use. SFMS processes financial transactions and provides financial information for most state agencies. Furthermore, SCD uses SFMS data to produce the state's comprehensive annual financial report.

During the fiscal year ended June 30, 1998, state agencies processed \$14 billion in revenues and expenditures through the system. SFMS operates on the DAS General Government Data Center mainframe computer. Although DAS is ultimately responsible for the overall integrity of SFMS, individual user agencies may customize certain system parameters to fit their organizational requirements or needs.

In April 1997, SCD implemented its Accounting Data Mart (data mart). The data mart is an ad hoc reporting facility containing weekly updates of selected SFMS data. The data mart permits agencies to generate customized reports to facilitate their decision-making. After two years of operation, the data mart contains approximately 60 million records representing over \$2.5 trillion in transactions. SCD works in cooperation with the General Government Data Center to control access to the data mart.

## **INFORMATION SYSTEMS CONTROLS**

Information system controls are generally categorized as general or application controls. General controls protect the environment in which all application software operates. Application controls are designed to reduce the risk of unauthorized, inaccurate, or incomplete input, processing, output, and storage of transactions for a specific application.

## **SCOPE AND METHODOLOGY**

Our application control review of the SFMS had the following objectives:

1. Determine if the controls over SFMS and the Accounting Data Mart (data mart) appropriately restrict access and adequately protect the system and data from unauthorized creation, use, damage or loss.

2. Determine if the controls over the data mart are adequate to ensure that the data in the warehouse completely and accurately reflect the information in SFMS.
3. Review the status of findings and recommendations reported in previous audits.

We performed our fieldwork between August 1998, and April 1999. We conducted our work in two phases, a preliminary risk assessment, and tests of selected system controls. Our preliminary risk assessment included identifying controls designed into the application or established by SFMS management, as well as assessing the risks that would be mitigated by these controls. We inquired of agency personnel, and reviewed system and user documentation and the work of the DAS Information Systems internal auditor.

Based on the results of our risk assessment, we tested the controls over SFMS security, and data mart security and data integrity. We designed procedures to determine if the selected controls were working as intended. We reviewed security records provided by the DAS and reviewed processes for updating the data mart. In addition, we compared data stored in the data mart with that stored in SFMS for a sample of agencies.

During our audit we used the Information Systems Audit and Control Foundation's (ISACF) Control Objectives for Information and Related Technology (COBIT) to identify generally accepted and applicable control objectives and practices for information systems. ISACF is a worldwide organization dedicated to researching and promulgating generally accepted information systems control objectives and audit guidelines. We conducted our audit in accordance with generally accepted government auditing standards.

## AUDIT RESULTS

### ACCESS CONTROLS

The Department of Administrative Services (DAS), State Controller's Division (SCD) is responsible for safeguarding the Statewide Financial Management System (SFMS) information against unauthorized use, disclosure or modification, damage or loss. SCD relies on IBM's Resource Access Control Facility (RACF) software to restrict access to the systems, data, and programs stored on the DAS mainframe, including SFMS. SCD uses security profiles within SFMS to further restrict which program screens or specific access privileges individuals can use.

The effectiveness of these access control mechanisms depends on whether they are properly implemented, maintained, and monitored. To ensure this, access to SFMS should be granted according to the individual's demonstrated need to view, add, change or delete data. In addition, changes to user security profiles should be properly authorized and documented and managers should have processes to regularly review and validate existing users' access privileges.

#### *Access Control Weaknesses*

The State Controller's Division could improve its control over access to SFMS. Specific access control weaknesses include the following:

- SFMS security profiles are not maintained in a timely or consistent manner.
- SCD does not have adequate processes and procedures for assigning and maintaining access privileges for temporary or non-standard users.
- Periodic reviews to confirm and evaluate existing user access privileges are not always effective.

SFMS security profiles define the screens or privileges granted to each user. Proper maintenance of SFMS access controls includes deactivating RACF User IDs and any associated security profiles when users leave state employment or assume different job responsibilities. Procedures to ensure that the above processes are accomplished are not always effective. For example, during our audit period we noted that 48 User IDs still

had security profiles even though their associated RACF User IDs were deactivated. One of these RACF User ID's was improperly reactivated after the employee was transferred to another agency.

SCD established special procedures for granting access for non-standard users of SFMS. These users include contractors, temporary employees, and others requiring some specific agency access privileges. However, many of the controls SCD uses to monitor and maintain normal SFMS access were not always effective for non-standard users. Specifically, we noted that many of those special User ID's were not properly deleted after they were no longer needed. In addition, one agency manager inappropriately requested a non-standard User ID for a fictitious user. During an 18-month period several agency employees entered transactions using this User ID. Even though the transactions entered using this User ID appeared to be authorized by other agency employees, it could not be determined which employees actually used the ID. Thus, its use circumvented controls intended to prevent fraudulent or unauthorized transaction from occurring.

SCD relies on semi-annual reviews to monitor access privileges. During these semi-annual reviews, SCD asks security officers from individual agencies to verify whether the security profiles assigned to their users are appropriate. Although these reviews involved agency security officers who are in a better position to determine whether security profiles for their agency's employees are appropriate, these reviews are not always effectively conducted. In some instances, agency security officers did not perform thorough reviews, and some did not communicate their results to SCD so that errors could be corrected. To determine the effectiveness of these reviews, we tested 58 User IDs to determine whether they had appropriate access privileges. Of those, 18 had unnecessary or excessive access privileges and one should have been inactivated. These exceptions were in addition to the 48 User IDs we identified during previous tests. In addition, agency security officers during their semi-annual reviews specifically approved several of the User IDs with inappropriate access privileges.

***Cause and Recommendations***

SCD is responsible for developing and communicating approved procedures to staff. Many of the above weaknesses were the result of insufficient procedures or documentation. For example, SCD employees did not have procedures for

retaining authorizations for access changes. In addition, its procedures for granting and maintaining access for non-standard SFMS users were inadequate to ensure those user's access privileges remained valid. Furthermore, policies and procedures are not sufficient to ensure agency security officers understand and carry out their responsibilities to control access.

These conditions increase the risk of unauthorized access to SFMS transactions or data. Thus, SCD is less able to protect its system and agency data from unauthorized use, disclosure or modification, and damage or loss.

**We recommend** that SCD management further develop and implement policies and procedures to improve access controls, including the following:

- Retain documentation of changes to SFMS User IDs in a manner that facilitates better monitoring of access controls.
- Establish procedures to ensure timely and consistent maintenance of SFMS User IDs.
- Establish effective methods for granting and maintaining non-standard user access privileges.
- Implement procedures to ensure more thorough semi-annual reviews of user access privileges, including procedures to ensure that agency security officers adequately understand security issues, respond to the reviews, and provide appropriate feedback to SCD.

## **DATA MART OPERATIONS AND MAINTENANCE**

SCD management is responsible for developing and implementing policies and procedures governing data mart operations and maintenance. These policies and procedures should provide specific guidance to ensure that data mart files accurately reflect the transactions in SFMS, and that important system functions are performed regularly and in an orderly fashion.

During our review we performed tests to verify whether SCD correctly copied SFMS source data to data mart files for the period July 1998 through December 1998. For the sample agency data we tested, data mart files accurately reflected the corresponding transactions in SFMS.

SCD has not developed written policies and procedures relating to data mart access control, billing, or operations. Thus, it relies on the personal knowledge and expertise of its staff to ensure that these functions occur as intended. As a result, SCD has increased its risk of errors occurring during data mart operations. In addition, lack of written procedures may impair data mart operations in the event of a change in personnel.

**We recommend** that SCD in conjunction with DAS Information Resources Management Division establish written policies and procedures to guide performance of data mart operations and billing, ensure system security, and maintain data integrity.

## **STATUS OF PRIOR AUDIT ISSUES**

Since July 1995, three audit reports relating to the SFMS have been issued. These reports include report number 95-26 issued July 17, 1995, report number 97-69 issued July 8, 1997, and report number 98-39 issued October 27, 1998.

Of the findings relating to SFMS included in these reports, 12 have been resolved satisfactorily and eight have been partially resolved. Two findings remain unresolved. The unresolved issues include not routinely conducting disaster recovery testing and not adequately restricting physical access to the DAS General Government Data Center. A table outlining the disposition of prior audit findings is found in **Appendix A** of this report.

To mitigate the risks associated with these weaknesses, **we recommend** that DAS fully resolve all outstanding prior audit issues.

## **COMMENDATION**

The courtesies and cooperation extended by officials and employees of the Department of Administrative Services during the course of this review were commendable and sincerely appreciated.

## **AUDIT TEAM**

Nancy Buffinton-Kelm, CPA, CISA

Neal Weatherspoon, CPA, CISA

Mark Winter, CPA, CISA

Nancy Winston, CPA, CISA

Jamie Breyman

Michael Clark



## SUMMARY OF PRIOR AUDIT FINDINGS

### Prior Audit Finding

### Current status

**Report:** *Agreed-Upon Procedures Report for the Statewide Financial Management System, Report 95-26, July 17, 1995.*

- |   |  |
|---|--|
| 1. Consolidate multiple change request forms into a single form.                                      | Resolved   |
| 2. Ensure Problem Report forms are properly completed   | Resolved   |
| 3. Restrict access to production region to support adequate segregation of duties                     | Resolved   |
| 4. Use available Panvalet facilities  | Resolved   |
| 5. Improve technical documentation.   | Resolved   |
| 6. Document the state's software maintenance responsibilities and liabilities for ADPICS and R*STARS. | Resolved   |
| 7. Ensure adequate understanding of the applications prior to KPMG departure.                         | Resolved   |
| 8. Document all ABEND's along with resolution.  | Resolved   |
| 9. Monitor DB2 activity   | Partially resolved. The agency has taken limited measures to reduce the number of individuals DBA authority, but does not monitor activity as recommended. |
| 10. Regularly update and test the disaster recovery plan.   | Unresolved   |
| 11. Strengthen controls over warrant distribution at State Printing Office                            | Resolved   |
| 12. Create an R*STARS interface for canceling posted vouchers   | Partially resolved. The agency has taken limited measures but deferred further work due to Y2K efforts.  |
| 13. Create the ability to cancel a direct voucher in ADPICS   | Partially resolved. The agency has taken limited measures but deferred further work due to Y2K efforts.  |

**Prior Audit Finding**

**Current status**

- |   |   |
|---|---|
| 14. Create the ability to record credit memos in ADPICS                             | Partially resolved. The agency has taken limited measures but deferred further work due to Y2K efforts.               |
| 15. Create transaction detail reports to ensure completeness and accuracy of input. | Partially resolved. The agency has taken limited measures but deferred further work due to Y2K efforts.               |
| 16. Create reports to ensure completeness and accuracy of update.                   | Partially resolved. The agency has taken limited measures but deferred further work due to Y2K efforts.               |
| 17. Functions not currently in production.  | Partially resolved. SFMS management has completed testing for Purge and ACH, but has not yet implemented the modules. |
| 18. Review access to R*STARS system-wide tables and parameters.                     | Resolved  |
| 19. Enforce change control procedures for system-wide tables and parameters.        | Resolved  |

**Report:** *Statewide Financial Management System – Special Review, Report 97-69, July 8, 1997.*

- |               |  |
|---------------|--|
| 20. Year 2000 | Resolved   |
| 21. STARGAZE  | Partially resolved. No decision on the implementation of this graphical user interface has been made; however, software maintenance payments were stopped in 1997 for this software. |

**Report:** *Department of Administrative Services (DAS): Computer Center General Controls Review, Report 98-39, October 27, 1998.*

- |  |            |
|--|------------|
| 22. The Information Resources Management Division has not established policies requiring visitor escort or logging of computer center visitors. It has not provided sufficient physical security of the state's data center. | Unresolved |
|--|------------|

**AGENCY'S RESPONSE TO THE AUDIT REPORT**





# Oregon

John A. Kitzhaber, M.D., Governor

## Department of Administrative Services

Office of the Director  
155 Cottage Street NE  
Salem, OR 97310-0310  
(503) 378-3104  
FAX (503) 373-7643

November 15, 1999

To: Sharron E. Walker, Deputy Director  
Audits Division, Secretary of State

Jon Yunker, Director  
Department of Administrative Services

Subject: **Response to Statewide Financial Management System Application Controls Audit Findings**

Thank you for your letter of October 22, 1999 notifying the Department of Administrative Services of your findings and recommendations for the Statewide Financial Management System (SFMS). The conditions were identified in the SFMS Application Controls Audit performed from August 1998 to April 1999. Our response to each specific recommendation follows:

### **Current Audit Findings:**

*The State Controller's Division (SCD) further develop and implement controls and procedures to improve access controls.*

The SCD generally agrees with this finding. We have improved our process for maintaining documentation of security changes. Requests are filed both electronically and in paper form by agency to facilitate monitoring of access controls. We have developed reports to query security data to ensure more timely and consistent review and maintenance of user IDs. By June of 2000, we expect to have our internal procedures documented, including criteria for establishing non-standard access privileges. In addition, we will implement a policy by June of 2000. The policy will provide guidance for agency security officers. We will continue to provide training to agency security officers to provide information and guidance on security issues. The training will also stress the importance of responding to our semi-annual security reviews. The Statewide Accounting and Reporting section is responsible for this item.

*The SCD in conjunction with IRMD establish written policies and procedures to guide performance of data mart operations and billing, ensure system security, and maintain data integrity.*

The SCD generally agrees with this finding. We plan to work with IRMD to document procedures for managing security over the data mart. We will also document the process used in verifying that the key elements of the data mart agree to SFMS production records. We expect to complete this documentation by June of 2000. The Statewide Accounting and Reporting section is responsible for this item.



IRMD generally agrees with the portion of the finding concerning the need to document billing processes. IRMD has developed two ISO 9000 Work Instructions related to the IRMD General Government Data Center (GGDC) billing system. The billing system includes billings for the Data Mart. Work Instruction #4224-09-0507 presents a detailed flowchart of the billing system. Work Instruction #4225-20-0521 provides procedures for updating and maintaining the billing system. Both Work Instructions were issued on June 30, 1999. The GGDC plans to write procedures for the manual portion of the billing processes no later than March of 2000. The GGDC Manager is responsible for this item.

**Prior Audit Findings Still Open:**

***Monitor DB2 activity.***

IRMD Systems Development and Consulting will work with the IRMD General Government Data Center and the DAS Internal Auditor to develop the recommended reports and procedures to provide for the routine review of unusual DB2 activity. We expect to implement the reporting and monitoring process by June of 2000.

***Regularly update and test the disaster recovery plan.***

IRMD agrees with the audit finding. IRMD's General Government Data Center is now performing its remote disaster recovery rehearsal for its mainframe computer system. The Data Center Manager plans to conduct these tests every two years.

The DAS/IRMD Network Communications Services (NCS) Section, Data and Video Unit, Network Operations Center (NOC) completed their Wide Area Network Disaster Recovery Plan on July 1, 1999. Although the plan is still in draft form, it will be followed in case of a disaster. The NCS NOC is using this disaster recovery plan for their Y2K Business Continuation Planning (BCP) process as well as a guide for their Y2K Table Top Exercises. The NCS NOC will continue to revise and add to the disaster recovery planning process as provided within the context of our ISO-9001 procedures. The plan will be formally finalized before December 31, 1999. The NCS Data and Video Services Manager is responsible for this action.

***Create an R\*STARS interface for canceling posted vouchers.***

Change Request (CR) 206 was developed to address this concern and is still open. All work on changes was stopped during testing and revisions for Y2K needs. We have not yet resumed the review of the change requests. This CR is prioritized below required Purge changes and other functionality needs. We plan to evaluate this CR by June 30, 2001 and prioritize it along with other programming activities. The SFMS Services Unit is responsible for this item.

***Create the ability to cancel a direct voucher in ADPICS.***

CR206 was developed to address this concern and is still open. All work on changes was stopped during testing and revisions for Y2K needs. We have not yet resumed the review of the change requests. This CR is prioritized below required Purge changes and other functionality needs. We plan to evaluate this CR by June 30, 2001 and prioritize it along with other programming activities. The SFMS Services Unit is responsible for this item.

***Create the ability to record credit memos in ADPICS.***

CR205 was developed to address this concern and is still open. All work on changes was stopped during testing and revisions for Y2K needs. We have not yet resumed the review of the change requests. This CR is prioritized below required Purge changes and other functionality needs. We plan to evaluate this CR by June 30, 2001 and prioritize it along with other programming activities. The SFMS Services Unit is responsible for this item.

***Create transaction detail reports to ensure completeness and accuracy of update.***

CR207 was developed to address this concern and is still open. All work on changes was stopped during testing and revisions for Y2K needs. We have not yet resumed the review of the change requests. This CR is prioritized below required Purge changes and other functionality needs. We plan to evaluate this CR by June 30, 2001 and prioritize it along with other programming activities. The SFMS Services Unit is responsible for this item.

***Create reports to ensure completeness and accuracy of update.***

CR207 was developed to address this concern and is still open. All work on changes was stopped during testing and revisions for Y2K needs. We have not yet resumed the review of the change requests. This CR is prioritized below required Purge changes and other functionality needs. We plan to evaluate this CR by June 30, 2001 and prioritize it along with other programming activities. The SFMS Services Unit is responsible for this item.

***Functions not currently in production.***

SFMS management has completed Y2K testing for Purge and ACH. We have begun preparations for implementation of Purge, our number one priority for the next year. Since both Purge and ACH are major projects, ACH will remain "on hold" until Purge and other higher priority functionality needs are resolved. We do not have the staff resources to do both projects at the same time and we have not yet set a completion date for implementing ACH. The SFMS Services Unit is responsible for this item.

***STARGAZE.***

We have not yet conducted a formal cost/benefit evaluation of this graphical user interface tool. This project has been delayed because of Y2K testing and is prioritized below required Purge changes and other functionality needs. Although originally expected to be evaluated sooner, we do not reasonably envision any work being done on this project before Purge is completed in late 2000. We plan to review this priority by June 30, 2001. The SFMS Operations Unit is responsible for this item.

***IRMD has not established policies requiring visitor escort or logging of Computer Center visitors. It has not provided adequate physical security of the state's data center.***

IRMD agrees with the audit finding. Controlling access to the Data Center is a top priority for IRMD. A management vacancy for almost one year has put us behind in implementing our corrective plan. However, some progress has been made. A visitors log is now being used. All Data Center visitors sign

Response to Audit Conditions and Recommendations  
August 12, 1999

in on the log, receive a badge and are escorted to the Data Center. The current design of the facility makes it difficult to control visitors. IRMD will contact Facilities to examine the feasibility of placing a receptionist near the entryway. The receptionist will require visitors to sign-in, pick up a badge and be escorted into the various IRMD sections. In addition, IRMD will evaluate its FTE to locate staffing resources to support the receptionist desk. A visitor access policy will be developed and adopted. These actions will be completed not later than March 2000. IRMD is responsible for this item.

Thank you for your time over the past few months to review the SFMS application controls. If you have any questions or need additional information, please call Valerie Wicklund at 378-3742.

## **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*

*Deputy Director*

*Deputy Director*

John N. Lattimer

Catherine E. Pollino, CGFM

Sharron E. Walker, CPA, CFE



This report, which is a public record, 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/auditthp.htm>

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