



Secretary of State Audit Report

Oregon Department of Transportation: TEAMS Application Controls Review

Summary

PURPOSE

The purpose of this audit was to determine whether controls governing the Oregon Department of Transportation (department) Transportation Environment Accounting and Management System (TEAMS):

- Provided reasonable assurance that expenditure transactions were completely recorded, properly authorized, accurately processed, properly classified by fiscal period, and protected to maintain data integrity;
- Ensured that system data and program files were reasonably protected from unauthorized viewing, modification, or deletion; and
- Provided reasonable assurance that only properly approved and tested changes to program code were used during processing.

RESULTS IN BRIEF

Controls governing TEAMS during the scope of our audit provided reasonable assurance that expenditure transactions were completely recorded, properly authorized,

accurately processed and properly classified by fiscal period.

However, logical access to production programs and data was not monitored to ensure that access was granted only to individuals with a demonstrated need for such access.

In addition, controls governing emergency changes to TEAMS did not ensure that managers were aware when emergency modifications occurred or temporary fixes timely replaced with approved code.

RECOMMENDATIONS

We recommend that department management routinely re-evaluate and adjust logical access to TEAMS production files and data and modify its program change management procedures to adopt more robust monitoring of emergency changes to production programs.

AGENCY RESPONSE

The Oregon Department of Transportation generally agrees with the recommendations.

Background

Introduction

The Oregon Department of Transportation's (department) mission is to provide Oregonians with a safe, efficient transportation system that supports economic opportunity and livable communities.

The department's Transportation Environment Accounting and Management System

(TEAMS) serves as its main financial accounting system. This system processes financial and statistical information and reports financial and managerial information. It acts as a subsidiary system for processing payments, billings, and receipts. It also serves to track the costs and revenues for individual pro-

jects. TEAMS expenditures interface at a summary level with the Statewide Financial Management Application for financial reporting purposes.

Information System Controls

Information system controls are typically classified

Background (continued)

as general controls or application controls. General controls protect the environment in which software applications process data. Application controls relate to specific processing requirements

of individual software applications. These controls help ensure that transactions occur and are authorized and completely and accurately recorded and processed. Application controls coupled

with general controls provide increased assurance that transactions processed through the system are authorized, reliable, and complete.

Audit Results

Application Controls Ensure TEAMS Data Integrity

Controls governing the Transportation Environment Accounting and Management System (TEAMS) provided reasonable assurance that expenditure transactions were completely recorded, properly authorized, accurately processed, properly classified by fiscal period, and protected to maintain integrity.

We based the above conclusions on the results of various tests of data integrity. Some of the more significant results of those tests include the following:

- All checks written from TEAMS for a selected day's transactions were supported by transactions recorded within the system.
- All expenditure transactions that generated checks in our review period were authorized for processing in the system. In addition, someone other than the individual who entered those transactions performed the authorizations.
- Sample transactions' expenditure classifications, amounts, fiscal period and other critical data elements entered by the users remained unaltered through processing or were corrected as required.
- Processing edits to detect duplicate payments performed as expected.

- The design of TEAMS security is structured to restrict user access to specific application screens.
- Individuals who entered or approved non-interfaced expenditure transactions occurring during our testing period were authorized to perform those tasks.

Logical Access to Production Files Should Be More Closely Monitored

As discussed above, TEAMS security provisions provided reasonable assurance that staff entering or approving transactions through the system were authorized. To provide assurance that production programming and data files could not be accessed or altered by means outside of program control, the department utilized security software to password-protect those files.

The effectiveness of this "file-level" security is contingent on the department's diligence in ensuring file-level access is only given to individuals having a demonstrated need to view or modify those files outside of TEAMS program control. Generally accepted security controls also require that management periodically review, confirm, and adjust access rights to ensure users' access privileges continue to be justified.

During our review of access to TEAMS production files, we noted that two user groups, containing a total of 15

users, had unjustified access. According to a department manager, much of this access should have been removed during a clean-up project several years previously. In addition, he indicated access to TEAMS production files was not routinely evaluated. When we communicated the inappropriate access to the manager, he promptly ensured that it was removed.

Unjustified access to production files increases the risk that unauthorized transactions could be introduced into the processing stream or that the integrity of program and data files could otherwise be compromised.

We recommend that department management ensure that access to TEAMS production files is routinely re-evaluated and adjusted to include only those individuals having a demonstrated need for such access.

Agency's Response:

We agree with this recommendation. We will begin regular reviews of all groups having access to TEAMS data, as well as the membership in those groups.

Additional Program Change Management Procedures Should Be Adopted

Making changes to program code outside of the normal change management process is sometimes necessary to resolve problems encountered during

Audit Results (continued)

processing. These emergency changes should be closely monitored and subsequently subjected to normal change management requirements before they are elevated to permanent production status.

The department's change management procedures were generally adequate to ensure only properly approved and tested code was moved into production. However, the department's processes did not adequately ensure that emergency changes were necessary, closely monitored or timely replaced with code that passed normal change management requirements.

The department periodically produced reports indicating which emergency fixes were then in the system; however, those reports were not distributed to managers responsible for TEAMS maintenance.

The above weakness increases the risk that unauthorized code could be temporarily introduced and run in production.

We recommend that department management adopt procedures to more closely monitor emergency changes to TEAMS to ensure that those changes are necessary and timely replaced with

code that passed normal change management processes.

Agency's Response:

We agree with this recommendation. Financial Services will develop formal written procedures and standards for documenting and monitoring emergency fixes. Management will closely monitor emergency changes and make certain that reports are reviewed in order to guard against unauthorized code changes.

Objectives, Scope and Methodology

This objectives of this audit were to determine whether:

- Controls built into TEAMS provided reasonable assurance that expenditure transactions were completely recorded, properly authorized, accurately processed, properly classified by fiscal period, and protected to maintain their integrity.
- The department's file-level security was adequate to ensure that TEAMS data and program files were protected from unauthorized viewing, modification, or deletion.
- Controls over changes to TEAMS programs ensured that only properly approved and tested code was moved into the production region.

We limited our audit work to expenditure transactions posted to TEAMS for the dates July 1, 2002 through June 23, 2003 and the controls associated with those transactions. Testing of screen level security was conducted using data from July 1, 2002 through December 31, 2003.

During our audit, we interviewed department personnel responsible for using and maintaining the system to identify the controls associated with expenditure transactions. We also examined documents supporting controls and individual transactions. In addition, we analyzed electronic data to ensure transactions properly flowed through the system and controls functioned as intended.

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. ITGI is a worldwide organization dedicated to research, develop, and publicize control objectives and audit guidelines.

We conducted our audit according to generally accepted government auditing standards. We also conducted our audit according to Information Systems Audit and Control Association standards for information systems auditing.



Secretary of State
Audits Division

BILL BRADBURY, SECRETARY OF STATE
CATHY POLLINO, STATE AUDITOR, AUDITS DIVISION

255 Capitol St. NE Suite 500
Salem, OR 97310

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

AUDIT ADMINISTRATOR: *Neal E. Weatherspoon, CPA, CISA*

AUDIT STAFF: *Mark A. Winter, CPA, CISA*
Olivia M. Meyers

DEPUTY DIRECTOR: *Charles A. Hibner, CPA*

*The courtesies and cooperation extended by the officials and staff of the
Oregon Department of Transportation were commendable and much appreciated.*

*This report, which is a public record, is intended to promote the best possible
management of public resources. Copies may be obtained by mail at:*

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

*by phone at 503-986-2255 and 800-336-8218 (hotline), or
internet at Audits.Hotline@state.or.us and
<http://www.sos.state.or.us/audits/audithp.htm>*