



# Secretary of State Audit Report

## Department of Corrections: Automated Financial Accounting Manufacturing Inventory System Computer Controls Review

### Summary

#### PURPOSE

The Department of Corrections (department) was established by the Oregon Legislature in 1987. The department uses the Automated Financial Accounting Manufacturing Inventory System (system) as its main financial computer application. The system is currently hosted at the Department of Administrative Services State Data Center.

The purpose of this audit was to evaluate the effectiveness of key 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

We found that:

- Application controls provided reasonable assurance that information entered into the system would remain complete, accurate, and valid.
- The department had not fully implemented formal change management procedures, applied System Development Life Cycle (SDLC) methodologies to appropriately address pending system obsolescence issues, or assigned a system owner responsible for making important system development decisions.
- Department staff ensured regular backup tapes of critical system files were created. However, the department did not have a comprehensive plan for restoring the system in the event of a disaster. One particular item missing was a written service level agreement with the State Data Center clarifying each party's disaster recovery roles, responsibilities, and requirements.

- Security control weaknesses increased the risk that the system and its data could be compromised. Because of the sensitive nature of system security, we communicated these issues in a confidential report that included recommendations to improve security. That report was prepared in accordance with ORS 192.501 (23), which exempts such information from public disclosure.

#### RECOMMENDATIONS

We recommend that department management:

- fully implement formal program change management procedures, apply SDLC methodologies to address pending system obsolescence issues, and assign a system owner responsible for making important system development decisions;
- allocate sufficient resources to develop and test comprehensive disaster recovery procedures, including a written service level agreement with the State Data Center, to ensure timely restoration of the system in the event of a major disruption;
- implement the security recommendations included in our confidential security report; and
- formalize security expectations and requirements with the State Data Center using a written service level agreement and periodically obtain independent assurance that those expectations are being met.

#### AGENCY'S RESPONSE

The Department of Corrections generally agrees with the recommendations.

## Introduction

The Department of Corrections (department) was established by the Oregon Legislature in 1987. Its mission is to promote public safety by holding offenders accountable for their actions and reducing the risk of future criminal behavior.

The Automated Financial Accounting Manufacturing Inventory System (system) is the department's primary general accounting computer application. The system also provides financial information to the Statewide Financial Management Application and receives data from the Oregon State Payroll Application.

JD Edwards developed the system in the early 1990's and the department hired consultants to modify the system to better fit its needs. In 2001, the department committed to upgrade to the vendor's *OneWorld XE* version of the software. However, the department never fully implemented that version. As a result, during this audit the department's system configuration included a combination of the original *World* and newer *OneWorld XE* application modules.

*World* system modules reside on a mid-range (i-Series) computer platform. *OneWorld XE* modules reside on a separate *Windows* based platform. Both platforms are hosted at the Department of Administrative Services State Data Center.

## Purpose

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

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. These controls can be either manually operated or automated.

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

## Audit Results

### Application Controls Reasonably Ensured AFAMIS 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; that data integrity is maintained during processing; and that the system's outputs conform to anticipated results.

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

- transaction input;
- error detection and correction;
- agreement of subsidiaries and general ledger accounts; and
- the interface with the Statewide Financial Management Application.

Based on the results of these tests, we concluded that application controls provided reasonable assurance that information entered into the system would remain complete, accurate, and valid.

### Program Change Management Procedures Were Inadequate

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. In addition, organizations should have System Development Life Cycle (SDLC) methodologies to assess and define information system needs, consider alternative solutions, and determine the feasibility of proposed solutions.

Technical updates to system source code were provided by Oracle, a major software vendor. However, the department was responsible for making its own code changes to system interfaces and reporting structures. Oracle indicated it plans to discontinue support for the current *World* version of the system by 2013.

We evaluated the department's program change management controls and SDLC methodologies as they related to the system. We found the department had not:

- fully implemented formal change management procedures;
- applied SDLC methodologies to appropriately address pending system obsolescence issues; and
- assigned a system owner responsible for making important system development decisions.

These control weaknesses increase the risk that unauthorized system changes could occur. In addition, the department is less likely to successfully transition to a new system when that becomes necessary. Because acquisition and implementation of new systems require significant up-front planning and analysis, delaying these efforts would be inadvisable.

We identified similar control weaknesses during our 2005 audit of the system. They continued to exist because department management had not assigned sufficient priority or resources to resolve them.

We recommend department management fully implement formal program change management procedures, apply SDLC methodologies to address pending system obsolescence issues, and assign a system owner responsible for making important system development decisions.

**Agency's Response:**

*We agree that SDLC methodology should be fully implemented. Before the audit was completed, DOC had put program change management procedures and SDLC methodology in place. Information Technology projects, no matter how big or small, are required to follow the process. One individual is not able to put in a change process without controls. The assigned system owner for AFAMIS is the Assistant Director for General Services.*

*For example, DOC had determined that the configuration of World and OneWorld could not work with the upcoming Vista operating system installation (projected to be in the spring of 2009). A group of AFAMIS support staff, representing Information Technology and Fiscal Services, created an option paper with a recommendation that was presented to the system owner for approval. Since completion of the fieldwork for this audit, DOC has implemented the decision to upgrade World and discontinue using OneWorld. A project manager was assigned and the system owner was kept up to date with budgets and status reports.*

*As discussed above, SDLC methodologies were used to address the current system issues as they related to the Vista operating system. Contingent upon*

*funding, DOC still plans to do a feasibility study using SDLC methodology to deal with the obsolescence of World in the future.*

**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.

We reviewed the department's backup and restoration procedures and found that staff ensured regular backup tapes of critical system files were created. However, the department did not have a comprehensive plan for restoring the system in the event of a disaster. It also did not have a written service level agreement with the State Data Center clarifying each party's disaster recovery roles, responsibilities, and requirements.

We identified similar weaknesses during our 2005 audit of the system. In response to that audit, department managers indicated they had projects in place to resolve these issues by the end of that year. However, those projects did not occur as planned.

As a result of these weaknesses, timely or successful restoration of the system in the event of a major disruption would likely be problematic.

We recommend that the department allocate sufficient resources to develop and test comprehensive disaster recovery procedures to ensure timely restoration of the system in the event of a major disruption. Those procedures should include a written

service level agreement with the State Data Center to clarify critical disaster recovery roles, responsibilities, and expectations.

**Agency's Response:**

*We agree. DOC is taking a holistic approach to Business Continuity (BCP) and Disaster Recovery. DOC has an assigned project manager for BCP, and is working on plans throughout the department for disaster recovery needs and related BCP workarounds. At this point in the project, we are still evaluating which, if any, applications DOC will bring up and in what priority. We agree that we need to work with the State Data Center (SDC). As we finish up our DOC BCP, we need to communicate to SDC our plans and how we would operate. One of our next steps in the BCP project is to define a disaster recovery plan for restoring critical information within defined time constraints.*

**Security Controls Did Not Adequately Protect the System**

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 includes logical access controls to ensure system assets are further protected against unauthorized use, disclosure, modification, damage, or loss.

When organizations rely on external service providers to host their applications they should have formal service level agreements defining each party's specific expectations in carrying out these responsibilities. In addition, they should periodically obtain independent assurance that these security requirements are being met.

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.

We noted that logical access to system screens was primarily controlled through program code that limited access to data and resources based on information stored in user account profiles. Accordingly, we evaluated the department's processes for granting and managing user account profiles. In addition, we tested user profiles to determine whether they supported internal controls. Furthermore, we reviewed other controls that protected system files and data from access not initiated through the application.

We found that the above security controls did not always protect the system against unauthorized use, disclosure, modification, damage, or loss. In addition, on August 6, 2008, we issued a 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 system. Within that report, we identified specific security weaknesses relating to the computing environment at the data center.

While the department relies on the State Data Center to provide a safe computing environment to host the system, it did not have a written service level agreement defining each party's specific expectations in carrying out these responsibilities. In addition, the department did not obtain independent assurance that security expectations were being met.

The above security control weaknesses increased the risk that the system and its data could be compromised.

Because of the sensitive nature of system security, we communicated these issues to the department in a confidential report outlining specific details of our findings, as well as recommendations to improve security. We prepared that report in accordance with ORS 192.501 (23), which exempts such information from public disclosure.

**We recommend** that department management implement the security recommendations included in our confidential security report.

***Agency's Response:***

*We agree. DOC has received the report and will be working on a separate response to those recommendations.*

**We also recommend** that department management formalize security expectations and requirements with the State Data Center using a written service level agreement. It should also periodically obtain independent assurance that those expectations are being met.

***Agency's Response:***

*We agree. We will work with the State Data Center.*

## Objectives, Scope and Methodology

The purpose of our audit was to evaluate the effectiveness of key general and application controls for the department's Automated Financial Accounting Manufacturing Inventory System (system).

Our specific audit objectives were to determine whether the department had implemented controls to ensure:

- system data remained complete, accurate and valid during input, processing, and output;

- the system was reasonably protected against unauthorized use, disclosure, modification, or loss;
- system program modifications followed approved system development processes and change management procedures; and
- system services would be available as required in the event of a major disruption.

To accomplish our objectives, we interviewed various department personnel, examined documents supporting controls, and used standard query tools to analyze electronic data.

To test the application controls over data integrity, we made inquiries of agency staff, observed data input processes, and reviewed reconciliations.

To determine whether the application and its data were reasonably secure, we made inquiries of agency staff, reviewed security settings, and reviewed the level of access granted to selected department staff.

We tested system change management controls by interviewing department staff and reviewing the documentation associated with selected system changes.

To evaluate the back-up and recovery process, we interviewed department and State Data Center staff, and reviewed documentation for selected back-up processes.

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 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.



**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 Weatherspoon, CPA, CISA, CISSP*

AUDIT STAFF: *Katherine Riley, CISA  
Mark A. Winter, CPA, CISA*

DEPUTY DIRECTOR: *William K. Garber, CGFM, MPA*

*Courtesies and cooperation extended by officials and staff of the  
Department of Corrections 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:*

*Internet: <http://www.sos.state.or.us/audits/index.html>*

*Phone: at 503-986-2255*

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