Report No. 2005-04

January 14, 2005

Department of Corrections: AFAMIS Application Controls Review

Bill Bradbury, Secretary of State

Cathy Pollino, State Auditor, Audits Division

Secretary of State Audit Report

Summary

PURPOSE

The Department of Correction's (department) Automated Financial Accounting Manufacturing Inventory System (AFAMIS) is its main financial computer application. The purpose of this audit was to evaluate the effectiveness of computer controls governing AFAMIS, including system development, security, data integrity, and disaster recovery and contingency planning.

RESULTS IN BRIEF

Department management did not use generally accepted controls for system development and maintenance. In addition, many critical system development phases and processes were not adequately performed during the department's project to upgrade to the OneWorld XE version of the system. As a result, the system was in a general state of disrepair and the department's project to upgrade AFAMIS was in jeopardy of failure. In addition, during our review we identified approximately $177,000 in contract payments that were made contrary to state contracting rules.

Controls to secure AFAMIS programs, data, and online functions were also insufficient and ineffective. Access to AFAMIS data and programs was not properly restricted and the department's ability to provide reliable internal control was limited. As a result, the integrity and confidentiality of the system was at significant risk of compromise. Details of security findings and recommendations were provided to the department in a confidential report in accordance with ORS 192.501 (23), which allows exemption of such information from public disclosure.

Application controls to ensure integrity of AFAMIS data files were inadequate. Key data files used by the department's AFAMIS implementation, and which will be utilized by its OneWorld XE version, were not always complete, accurate or valid. As a result, the department is less able to safeguard or manage its financial assets and resources and the financial information it provides to outside entities may not accurately reflect its operations.

The department also had not developed disaster recovery and contingency plans to restore AFAMIS or its critical business functions in the event of a disaster or major disruption.

RECOMMENDATIONS

We recommend that department management:

- Adopt comprehensive system development methodologies to govern changes to AFAMIS and seek guidance from the Department of Administrative Services to resolve information technology resource and expertise issues and explore system alternatives.
- Comply with state contracting rules and consult with the Department of Justice to resolve identified contract compliance issues.
- Take immediate action to implement recommendations to resolve security issues included in our confidential report.
- Develop and implement plans to establish data integrity for key data files and maintain that integrity once it has been achieved.
- Fully develop, test, implement and maintain disaster recovery and business continuity plans.

AGENCY'S RESPONSE

Department of Corrections management generally agrees with the recommendations.

Background and 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 department's Automated Financial Accounting Manufacturing Inventory System (AFAMIS) was purchased and implemented in the early 1990's and serves as its main financial accounting system. During our audit, AFAMIS had over 700 active user profiles.

AFAMIS interfaces with the Statewide Financial Management Application and the Oregon State Payroll Application through both manual and automated processes.

Prior to July 2004, the department's Business and Finance Division was responsible for the maintenance and operation of AFAMIS, and the Information Systems Services Division provided mainframe and network support. Subsequently, the department's newly formed General Services Division assumed responsibility for those functions.

JD Edwards, a national software company, developed AFAMIS and the department hired other consultants to modify the system to better fit its needs. In 1997, JD Edwards announced it would no longer support the World version of AFAMIS that the department implemented. As a result, in 2001 the department committed to convert to the vendor's OneWorld XE version of the software. Another software company, PeopleSoft, purchased JD Edwards in 2003 and announced it would not support OneWorld XE after February 2005.

As of September 2004, the department had not completed its conversion to OneWorld XE.

Audit Objectives, Scope and Methodology

The purpose of our audit was to evaluate the effectiveness of key general and application computer controls for the department's AFAMIS application.

Our specific audit objectives were to determine whether the department:

- Used comprehensive system development life cycle methodologies to control changes to the system.
- Ensured AFAMIS programs, data, and online functions were adequately secured.
- Implemented application controls to ensure AFAMIS data remained complete, accurate and valid during input, processing and output.
- Provided disaster recovery and contingency planning to ensure AFAMIS could be restored with minimal business impact after a disruption.

During our audit we interviewed various department personnel, examined documents supporting controls, and analyzed electronic data. We also evaluated compliance with applicable laws, rules and regulations pertaining to AFAMIS and our audit objectives. We performed our fieldwork between May 2003 and October 2004.

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

Audit Results

System Development and Maintenance of AFAMIS Was Unstructured and Problematic

During our audit the department was in the process of upgrading its AFAMIS application to the vendor's OneWorld XE version. Because of that development, we focused our work on the system development processes the department used during the upgrade as well as procedures to maintain the existing system.

Developing or acquiring information technologies to satisfy business needs is a necessary but high-risk activity. To properly develop, acquire and maintain computer applications requires significant resources including people, applications, facilities and other technologies. The processes for managing and controlling these resources should be part of a System Development Life Cycle (SDLC) methodology with defined phases that address application development and/or acquisition, deployment, maintenance and retirement.

Each phase of the SDLC is an incremental step that lays a foundation for the next phase. Following structured SDLC methodologies reduces the likelihood that disruptions, unauthorized alterations, or errors could be introduced during development. In addition, following formal SDLC methodologies throughout the life cycle helps ensure that applications will continue to satisfy business needs in the most efficient and economical manner until they are formally retired or replaced.

The IT Governance Institute has developed a maturity model for system development methodologies based on the Software Engineering Institute's Capability Maturity Model. The Software Engineering Institute is part of Carnegie Mellon University. The maturity model categorizes and describes controls over the processes of acquiring and maintaining application software. Some of the model's critical success factors include:

- Presence of formal, accepted, understood and enforced system development and maintenance methodologies.
- Strong senior management support for system development and maintenance methodologies.
- Existence of clear, understood and accepted information technology acquisition practices.
- An approach and effort expended that is proportionate to the business relevance of the application.

These critical success factors were notably absent in the department's system development approach. Department management indicated that they did not use formal SDLC methodologies for system development and maintenance. In addition, most critical system development phases and processes were not adequately performed during the department's project to upgrade to the OneWorld XE version of the system. The maturity model describes this approach to system development and maintenance as "Level 1" or "Initial/Ad Hoc".

Department staff also did not follow a formal project plan, or provide adequate project management during the OneWorld XE upgrade project. As a result, the project proceeded before project managers determined what tasks actually needed to be done, the feasibility of those tasks, how long they would take to complete, how much they would cost, or whether users could effectively use the system after implementation.

In addition, while reviewing the OneWorld XE upgrade, we noted several contract compliance issues. In one instance, the department paid approximately $8,000 for services performed before the existence of a valid contract, and approximately $24,000 for deliverables already paid for under "fixed fee" contract provisions. If those payments had been appropriate, total contract payments would have exceeded the contract "not-to-exceed" amount by approximately $30,000. In addition, approximately $145,000 was paid to another contractor for training, application development and other services associated with the upgrade to OneWorld XE without a valid contract.

The most significant consequences resulting from the department's informal approach to system development was that its AFAMIS World implementation had significant security and internal control weaknesses, data integrity issues, and notable operational inefficiencies. In addition, the department's project to upgrade AFAMIS to the OneWorld XE version was in jeopardy of failure, with little likelihood of being completed before February 2005, when PeopleSoft indicated it would discontinue support of the application.

As of March 30, 2004, the department spent approximately 89 percent of budgeted project funds or approximately $721,000, having implemented only two of its seven modules. One of those modules was not fully functional and the other was not being used.

Although these issues were symptomatic of the department's lack of SDLC methodologies and inadequate project management, many other factors contributed to the problem. One of the most significant was the department's insufficient allocation of information technology resources and expertise assigned to AFAMIS and the upgrade project. External limitations and forces from its software vendors also significantly added to the overall risk and complicated the department's decisions.

We recommend that department management adopt and apply comprehensive system development life cycle methodologies and project management strategies. In addition, department management should ensure that the most critical system development tasks or phases are successfully completed before proceeding further with the OneWorld XE upgrade project.

We also recommend that the department seek guidance and expertise from the Information Resources Management and State Controller's Divisions of the Department of Administrative Services to resolve information technology resource and expertise issues and explore system alternatives to address pending issues arising from PeopleSoft's decision to discontinue its support of the OneWorld XE application.

Agency's Response:

The Department of Corrections (DOC) agrees with the recommendation. In an effort to explore system alternatives, the department consulted with Solutions Consulting, LLC (a quality assurance contractor) earlier this year to review the project, consider options, identify weaknesses in the project, and make recommendations to the DOC. The study confirmed a number of valid criticisms regarding DOC's management of the project; as a result, the department is taking a more formal project management approach.

The department has implemented a comprehensive System Development Life Cycle (SDLC) methodology and plans to apply this methodology to all future information technology projects. The department will use information technology resources and expertise available from the Department of Administrative Services (DAS), as well as explore system alternatives through the completion of a comprehensive feasibility study.

The department restructured the project management effort by developing a "OneWorld Upgrade" steering committee to oversee the project. Also, a new project manager has completed an integrated project plan.

We also recommend that the department fully comply with state contracting rules and consult with the Department of Justice (DOJ) to resolve specific contract compliance issues identified.

Agency's Response:

The DOC agrees with the recommendation and will consult with the DOJ to resolve the contract compliance issues stated within the report.

AFAMIS Data and Programs Were Not Appropriately Safeguarded

Executive management is responsible for establishing an overall approach to security and internal control to ensure protection of resources and to maintain integrity of computer systems.

Key elements that should be addressed within the security framework include:

- Processes for identifying and classifying data and assigning levels of protection accordingly.
- Rules for granting user access to system resources to ensure an appropriate level of internal control allocated according to "least-access" principles.
- Logical access control technologies configured to link users and resources according to access rules.
- Procedures for managing user accounts to ensure timely action relating to requesting, establishing, issuing, suspending and closing user accounts.
- Mechanisms to monitor security activity to enable timely response to security incidents.

We concluded that the department's security framework to protect its system was inadequate. Specifically, the department had not provided adequate controls to ensure AFAMIS screens and functions were protected from unauthorized access, modification or loss. In addition, access to AFAMIS data and programs was not properly restricted at the system level.

As a result, the department's ability to award access to provide reliable internal control was limited and the integrity and confidentiality of the system was at significant risk of compromise.

Because of the sensitive nature of system security, we have issued a separate report outlining specific details of our findings as well as recommendations to improve security. That confidential report was prepared in accordance with ORS 192.501 (23), which allows exemption of such information from public disclosure.

We recommend that the department take immediate action to implement the recommendations included in our confidential report.

Agency's Response:

The DOC agrees with this recommendation. The department has taken immediate action, has implemented some of the issues, and will develop plans for implementing the remainder of the issues included in the confidential report.

Application Controls Did Not Ensure Integrity of Key AFAMIS Data Files

Application controls may consist of manual or programmed processes and include methods for ensuring that:

- Only complete, accurate and valid data are entered and updated in a computer system.
- Processing accomplishes the correct task.
- Processing results meet expectations.
- Data are maintained.

AFAMIS is a complex financial accounting and management application using numerous data files. In order for the system to function as intended, critical files must maintain integrity throughout data input, processing and output.

We concluded that the department did not employ adequate application controls to ensure integrity of its AFAMIS system. Therefore, key data files used by the department's AFAMIS implementation, and which will be utilized by its OneWorld XE version, were not always complete, accurate or valid.

Specific data file integrity issues included:

- Accounts payable and accounts receivable sub-ledger totals did not reconcile to general ledger totals.
- Transactions were inconsistently entered into expenditure accounts. We questioned the validity of account classifications for 24 of 33 expenditure transactions tested.
- Vendor master files contained numerous duplicate entries.

- Budget ledger files contained invalid user defined codes.
- Some transactions that were entered into the Statewide Financial Management Application (SFMA) were not entered into AFAMIS.
- The file containing purchasing and approving authority parameters was incomplete. Specifically, we selected a sample of 87 expenditures and found that 50 transactions were signed by individuals who were not included in the department's authority listing.

Some of the above data integrity issues occurred because staff was not always aware of how AFAMIS worked, what automated application controls were in place, or how controls functioned. Very few individuals understood the system sufficiently to answer even routine inquiries regarding AFAMIS data or data integrity issues. In some instances, only one individual could provide potential reasons for data abnormalities; in other instances, no explanation was offered. In addition, the department had not developed a functional chart of accounts to provide guidance to staff entering data so transactions would be posted to appropriate accounts in a consistent manner. Further, the department did not appropriately monitor important files to ensure they were reconciled and differences resolved.

Because of AFAMIS data integrity issues, the department is less able to safeguard or manage its financial assets and resources. In addition, the financial information it provides to outside entities may not accurately reflect its operations. For example, during a 2003 financial audit, various expenditure accounts were deemed unauditable because of posting errors and misclassifications.

We recommend that department management develop and implement plans to establish data integrity for key data files and maintain that integrity once it has been achieved. In doing so, it should:

- Establish more effective automated and manual error prevention, detection and correction controls.
- Ensure that staff responsible for AFAMIS has a comprehensive understanding of accounting and information system controls.
- Develop and implement a functional chart of accounts.
- Perform periodic reconciliations of AFAMIS account balances to ensure integrity within the system and to ensure that balances are accurately posted to SFMA.

Agency's Response:

The DOC agrees with the recommendation. It is important to note, however, that the data integrity issues are not related to the performance of the department's financial accounting software, but to the increased complexity of accounting transactions due to the growth of the department. To ensure data integrity, the department has developed and is implementing the following plan for key data files:

- *The department's controller is monitoring the update to the chart of accounts to ensure functionality. An Accountant 2 is currently updating the expenditures and inventory accounts in the chart of accounts.*
- *An Accountant 2 has been reassigned to reconcile AFAMIS to the Statewide Financial Management Application (SFMA) on a monthly basis to ensure that balances are accurately posted to the SFMA.*
- *An Accountant 1 was hired and is scheduled to begin employment with the department in January 2005. This position is responsible for reviewing and approving payments prior to input into AFAMIS to ensure data integrity.*
- *The department will hire an Accountant 3 with a start date of February 1, 2005. This position will be responsible for reviewing and reconciling certificates of participation and other funds information entered into AFAMIS and SFMA.*

Disaster Recovery and Business Continuity Planning Were Not Performed

Disaster recovery and business continuity planning are critical controls for safeguarding assets and ensuring the viability of the department's information systems and functions in the event of a major disruption. Ensuring that adequate disaster recovery planning occurs is the responsibility of senior management.

Important elements in disaster recovery and business continuity planning include:

- Performing a business impact analysis to identify time-critical aspects of critical business processes.
- Identifying and selecting appropriate recovery alternatives that meet the recovery time requirements.
- Developing, designing, and documenting detailed recovery strategies into written plans.
- Periodically testing chosen recovery strategies, maintaining the plan and ensuring that key people are aware and trained in their responsibilities.

Backup and offsite storage of critical system files is also a key

ingredient in recovering an information system after a significant event. Although the department was backing up AFAMIS programs and files, it had not developed disaster recovery and business continuity plans to restore the application or business operations in the event of a disaster.

Because the department performs a critical public safety mission, an inability or significant delay in recovering its systems or continuing business operations would pose an unacceptable risk.

We recommend that department management fully develop, test, implement and maintain disaster recovery and business continuity plans to better ensure timely recovery of critical systems and business functions.

Agency's Response:

The DOC agrees with the recommendation. The department initiated a project to complete a Business and Disaster Recovery Plan for all business functions and corresponding automated systems. The methodology being employed includes all the elements mentioned in this report. Major milestones are:

- *Development of a business impact analysis, scheduled for completion January 31, 2005.*
- *Identification and selection of recovery alternatives, scheduled for completion April 30, 2005.*
- *Finalization and documentation of the business continuity and disaster recover plan, scheduled for November 30, 2005.*

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: *Shandi C. Frederickson, CPA*
David T. Moon, CPA
Virginia L. Teller, CISA
Ben A. McClelland

DEPUTY STATE AUDITOR: *Charles A. Hibner, CPA*

The courtesies and cooperation extended by the 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 from our website *on the internet at:*
http://www.sos.state.or.us/audits/audithp.htm
by phone at 503-986-2255
or by mail from:
Oregon Audits Division
255 Capitol Street NE, Suite 500
Salem, OR 97310