COMPLIANCE AND CONTROL AUDIT REPORT

Department of Corrections: Reviewing the Adequacy of Its Controls Over Its Information Technology Systems

A Report to the Legislative Post Audit Committee
By the Legislative Division of Post Audit
State of Kansas
December 2001

01-D

Legislative Post Audit Committee
Legislative Division of Post Audit

The Legislative Post Audit Committee and its audit agency, the Legislative Division of Post Audit, are the audit arm of Kansas government. The programs and activities of State government now cost about $9 billion a year. As legislators and administrators try increasingly to allocate tax dollars effectively and make government work more efficiently, they need information to evaluate the work of government agencies. The audit work performed by Legislative Post Audit helps provide that information.

We conduct our audit work in accordance with applicable government auditing standards set forth by the U. S. General Accounting Office. These standards pertain to the auditor's professional qualifications, the quality of the audit work, and the characteristics of professional and meaningful reports. These audit standards have been endorsed by the American Institute of Certified Public Accountants and adopted by the Legislative Post Audit Committee.

The Legislative Post Audit Committee is a bipartisan committee comprising five senators and five representatives. Of the Senate members, three are appointed by the President of the Senate and two are appointed by the Senate Minority Leader. Of the representatives, three are appointed by the Speaker of the House and two are appointed by the House Minority Leader.

As part of its audit responsibilities, the Division is charged with meeting the requirements of the Legislative Post Audit Act which address audits of financial matters. Those requirements call for two major types of audit work.

First, the Act requires an annual audit of the State's financial statements. Those statements, prepared by the Department of Administration's Division of Accounts and Reports, are audited by a certified public accounting firm under contract with the Legislative Division of Post Audit. The firm is selected by the Contract Audit Committee, which comprises three members of the Legislative Post Audit Committee (including the Chairman and Vice-Chairman), the Secretary of Administration, and the Legislative Post Auditor. This audit work also meets the State's audit responsibilities under the federal Single Audit Act.

Second, the Act provides for a regular audit presence in every State agency by requiring that audit work be conducted at each agency at least once every three years. Audit work done in addition to the annual financial statement audit focuses on compliance with legal and procedural requirements and on the adequacy of the audited agency's internal control procedures. These compliance and control audits are conducted by the Division's staff under the direction of the Legislative Post Audit Committee.

LEGISLATIVE DIVISION OF POST AUDIT

800 SW Jackson
Suite 1200
Topeka, Kansas 66612-2212
Telephone (785) 296-3792
FAX (785) 296-4482
E-mail: LPA@lpa.state.ks.us
Website:
http://skyways.lib.ks.us/ksleg/PAUD/homepage.html
Barbara J. Hinton, Legislative Post Auditor

The Legislative Division of Post Audit supports full access to the services of State government for all citizens. Upon request, Legislative Post Audit can provide its audit reports in large print, audio, or other appropriate alternative format to accommodate persons with visual impairments. Persons with hearing or speech disabilities may reach us through the Kansas Relay Center at 1-800-766-3777. Our office hours are 8:00 a.m. to 5:00 p.m., Monday through Friday.

LEGISLATURE OF KANSAS

LEGISLATIVE DIVISION OF POST AUDIT

800 SOUTHWEST JACKSON STREET, SUITE 1200
TOPEKA, KANSAS 66612-2212
TELEPHONE (785) 296-3792
FAX (785) 296-4482
E-MAIL: lpa@lpa.state.ks.us

November 27, 2001

To: Members, Legislative Post Audit Committee

Representative Lisa Benlon, Chair	Senator Lynn Jenkins, Vice-Chair
Representative Richard Alldritt	Senator Anthony Hensley
Representative John Ballou	Senator Dave Kerr
Representative Dean Newton	Senator Derek Schmidt
Representative Dan Thimesch	Senator Chris Steineger

This report contains the findings, conclusions, and recommendations from our completed compliance and control audit of the *Department of Corrections: Reviewing the Adequacy of Its Controls Over Its Information Technology Systems.*

We would be happy to discuss the findings presented in this report with any legislative committees, individual legislators, or other State officials.

Barbara J. Hinton
Legislative Post Auditor

EXECUTIVE SUMMARY

LEGISLATIVE DIVISION OF POST AUDIT

Question 1: Has the Department Developed Adequate Policies To Ensure that Data in its Computer Systems Are Entered Accurately and Completely, and Reliably Maintained?

Because of the need to rely on data in computer systems, several layers of data quality controls are required to ensure data quality. *Without accurate data, managers can't make decisions with confidence. However, controlling data quality requires having controls over how data are collected and entered, monitored for mistakes as they are being entered, processed, and reported.* ..... page 5

The system we reviewed generally had good controls to ensure accurate data. *We found many of the types of controls we were looking for, and the controls built into the computer system that we tested generally worked well.* ..... page 6

The design of the system, and the lack of controls over data before they are entered, raises the risk of data entry errors. *While we found that the system's controls were generally good, we did find problems such as the following:* ..... page 6

- *The system doesn't allow someone to track a piece of data from the computer back to a source document, or to the person who entered it*
- *The way the system is designed allows data entry mistakes to be easily made*
- *Management in the facilities used few controls to protect data that were being entered*
- *The Department doesn't have training manuals or up-to-date user manuals for the system*

The age of the offender management system in general, and the inmate movement system in particular, increase the risk of system failure. *The Offender Management System was created in the late 1970s and is written in a programming language that fewer and fewer programmers are familiar with. In addition, like most programs of its age, the programming is poorly documented. These factors significantly raise the risk of a catastrophic failure of the System.* ..... page 8

Question 1 Recommendations ..... page 8

Question 2: Does the Department Adequately Manage the Maintenance and Updating of Its Critical Software?

Question 3: Has the Department Adequately Planned For the Actions It Must Take In the Event Of A Disaster To Minimize the Loss of Computer Operations?

computer functions that are most necessary to continued agency operations. Continuity planning enables an organization to minimize the loss of communications and important computer operations during an emergency.

The Department has done little business continuity planning for its critical computer programs. *Department management have implemented some sound practices, such as a system for backing up critical data. However, the Department doesn't meet many other planning standards. We found problems such as the following:*

- *The Department hasn't conducted a risk analysis to assess possible disaster scenarios or threats*
- *The existing continuity plan doesn't assign roles and responsibilities to specific staff, and is limited in the recovery instructions it gives*
- *The Department hasn't made any arrangements for off-site processing for its critical computer programs*

This audit was conducted by Allan Foster. Randy Tongier was the audit manager. If you need any additional information about the audit's findings, please contact Mr. Foster at the Division's offices. Our address is: Legislative Division of Post Audit, 800 SW Jackson Street, Suite 1200, Topeka, Kansas 66612. You also may call us at (785) 296-3792, or contact us via the Internet at LPA@lpa.state.ks.us.

Department of Corrections: Reviewing the Adequacy of ItsControls Over Its Information Technology Systems

The Legislative Division of Post Audit has conducted compliance and control audit work at the Department of Corrections. Compliance and control audits can identify noncompliance with applicable requirements and poor financial-management practices. The resulting audit findings often identify needed improvements that can help minimize the risk of potential future loss or misuse of State resources. This is the first of a series of specialized compliance and control audits designed to focus on an important area of agency operations that hasn't been reviewed–the technical aspects of operating information systems.

At the direction of the Legislative Post Audit Committee, this audit focused on the management of the Department's information systems. Specifically, we reviewed how the Department protects data quality, manages changes to its computer programs, and plans for disasters The audit addresses the following questions:

1. **Has the Department developed adequate policies to ensure that data in its computer systems are entered accurately and completely, and reliably maintained?**

2. **Does the Department adequately manage the maintenance and updating of its critical software?**

3. **Has the Department adequately planned for the actions it must take in the event of a disaster to minimize the loss of computer operations and has it adequately tested those plans?**

To answer these questions, we reviewed information system standards and best practices in each of the three areas listed above, interviewed Department officials, reviewed and evaluated policies and other documentation, and tested selected computer controls and edits used by the Department in managing its computer systems.

For reporting purposes, we've expanded the scope statement's one question into three.

The criteria we used in reviewing the Department's management efforts in these three areas were the Control Objectives for Information and Related Technology (COBIT), published by the Information Systems Audit and Control Association. These objectives are a set of high-level standards or best practices with a strong management orientation, which emphasize those controls that are necessary to ensure that information systems support the overall business objectives of an organization.

In conducting this audit, we followed all applicable government auditing standards. Our findings begin on page 5, following a brief overview.

Overview of the Department of Corrections Information Technology Division

The Department uses a wide range of computer technology in carrying out its responsibilities. The Department's computerized network currently supports eight correctional facilities and their satellites, more than 20 parole offices, and more than 29 community corrections offices. The Information Technology Division's IBM AS-400 mid-range computer houses most of the Department's critical computer programs. The Information Technology Division is responsible for planning, operation, and support of all the information technology functions in the Department, including telecommunications.

The Division's most important responsibility is to maintain several applications used to manage offender information. The Department uses that information to track each offender's progress through facilities, programs, community corrections, and parole. Most of that information is contained in two computer programs called the Offender Management Information System (OMIS), and the Total Offender Activity Documentation System (TOADS).

The Offender Management System contains data on all offenders sentenced to Department custody since it was developed in the late 1970s. The System contains demographics, sentencing information, good time awards, classification, location and movement information, work and program assignments, disciplinary history, parole decisions, grievances, and inmate banking records. It's the largest, and probably the most critical, computer system the Department manages.

The Total Offender Activity Documentation System is the supervision case management system for parole services and community corrections. The System contains data on demographics, sentencing and good time awards, supervision levels, risks and needs, location and status, employment, parole decisions, condition violations, sanctions and interventions, substance abuse testing, and supervision fees. It has been in use only about a year and the Department is still adding features to the system, such as developing better reporting and query functions so field staff can retrieve information faster.

The Division also operates systems to maintain digital photographs of offenders and is in the process of converting inmate records to digital images and storing them on computer. In addition, the Division is developing a system to provide information to the

Criminal Justice Information System (CJIS) on adult offenders supervised in the community, and is working with a contractor to develop an electronic medical records system. The Division also maintains the Department's network operations, and manages security for the network.

The Department of Corrections Information Technology Division

AT A GLANCE

Staffing: The Division has 43 full-time equivalent positions split between the central office and the correctional facilities.

Budget: The Division's funding comes primarily from the General Fund appropriations. The Division also receives moneys from the federal Edward Byrne Memorial Grant for work they do related to the Kansas Criminal justice Information System project.

FY 2001 Funding Sources

Total Funding: $3,931,982

FY 2001 Expenditures

Type	Amount	% of Total
Salaries/Wages	$1,802,572	46%
Contractual Services	751,402	19%
Commodities	410,650	10%
Capital Outlay	967,359	25%
Total Expenses:	**$3,931,982**	**100%**

Question 1: Has the Department Developed Adequate Policies To Ensure That Data in Its Computer Systems Are Entered Accurately and Completely, and Reliably Maintained?

The system we reviewed for this question, the Offender Management System, has good data quality controls to check for errors in data that's being entered. However, we did identify several problems. Managers in the facilities don't use good controls over data before it's entered into the computer system, the system has a poor audit trail for entered data, and the Department lacks user manuals. The outdated design of the system makes data entry errors more likely by requiring clerks to enter information using complex codes. Finally, the age of the system makes it fragile, presenting significant data risks to the Department.

Because of the Need To Rely On the Data In Computer Systems, Several Layers of Data Quality Controls Are Required To Ensure Data Quality

Data quality is extremely important to an agency. Without accurate data, or at least good assurance that data are accurate, managers are prevented from making decisions with confidence. In a worse case, managers unknowingly make incorrect decisions. In today's environment where nearly all decisions are based to some extent on computerized data, reliability is essential. Controlling data quality takes significant effort. Several layers of controls are needed, such as:

- controls over how the data is collected and entered into the computer to help avoid losing data or making other data entry errors
- controls or edits in the computer program to check the data being entered for obvious mistakes, such as letters in a field that's supposed to hold numbers, so that the person entering the data can correct it immediately
- controls in the actual processing of the data inside the computer to make sure data isn't lost or corrupted during the processing
- controls over the data that's output to make sure it doesn't go to people who don't have access to the data

Data quality is one of the more complicated areas of computer controls. Because of this complexity, we limited our review to the controls over data input and output.

We reviewed the controls in the Offender Management System for Question 1. When we began our review, we found that the Offender Management System is made up of many smaller programs, each of which has different controls. Therefore, we chose to review one of the components of the Offender Management System. We picked the Movement system because of its

importance. The Movement system is used to keep track of inmates, and for maintaining population counts in the facilities. Whenever an inmate moves from one cell block to another, or from one prison to another, an entry is made into the Movement system.

Some of the major data quality control areas specified in the COBIT standards are:

- supervisory approval of the preparation and entering of data before input
- controls that help ensure that transactions aren't lost or duplicated during data entry
- controls programmed into the computer that help ensure that input data is accurate
- development of an audit trail that allows transactions to be traced back to source documents
- controls that help ensure that output is correct

The System We Reviewed Generally Had Good Controls To Ensure Accurate Data

The data in the Offender Management System originates in the correctional facilities. Clerks gather information about inmate transfers, translate the information into codes that can be used by the computer, and enter the coded information into the computer. The computer system is programmed to check the data for accuracy. For example, if a clerk makes a typo in entering a code, and the number they enter isn't an allowable code, the computer won't accept the entry. When the clerk is done entering all the movement data, the computer provides a report that shows all the changes they made with that batch of entries. The clerk can use this report to check the accuracy of the entered data. In addition, output from the system is used daily to do inmate counts in the cell houses, and these counts act as data quality reviews.

We found many of the types of controls we were looking for, and found that the controls in this system were generally good. We tested many of the built-in edits, and they all worked well. We also talked to a sample of people in 2 correctional facilities who use the data, and they reported that the data in the system are generally accurate and useful.

The Design of the System, And the Lack of Controls Over Data Before They Are Entered, Raises the Risk of Data Entry Errors

While we found that the system's controls were generally good, we did find some problems. The most significant were:

The system doesn't allow someone to track a piece of data from the computer back to a source document, or to the person who entered it. This limits management's ability to investigate

problems, and makes it difficult to recreate entries that become lost or corrupted. Department officials told us that it would be extremely difficult to modify this system to accept such data because of the age of the system.

The way the system is designed allows mistakes to be easily made. The Movement system was developed in the late 1970's and uses antiquated methods of recording information. For example, much of the movement data must be transferred into complex codes for data entry. Here are a few of the 123 movement action codes staff must use to describe the reason for the move:

Code	Reason for Move
0301010	Par/CR Returned to KS Supervsn
0301020	DOC War. Wthdrwn Supervsn I/S
0301021	DOC War. Wthdrwn Supervsn O/S
0302010	Det. Par/CR Rtnd KS Supervsn
0302020	Det. Par/CR Rtnd O/S Supervsn

As you can see, choosing between 123 of these codes, and exactly entering the correct seven-digit number could be problematic. This particular example is doubly confusing. The clerk must first be able to understand the cryptic "Reason for Move," choose the proper code, then accurately enter the seven-digit code that differs little from the other codes surrounding it. Using such complex codes increases the risk of an incorrect code being entered. As mentioned above, the program will reject a code that isn't on the approved list of codes, but if a code that's wrong but on the approved list is chosen, the program has no way to know that the clerk has made a mistake.

We found that management in the facilities used few controls to protect data that was being entered. Generally, data entry forms weren't used, staff tended to code the data as it was being entered, and there was no supervisory review of the data before it was entered. In addition, there generally weren't ways to make sure that all the inmate movements were entered.

The Department doesn't have training manuals or up-to-date user manuals for the Movement system. Instead, staff rely on multi-page lists of allowable codes. This is a problem, especially if there were periods of high turnover in clerks in the correctional facilities. This is compounded by the complex nature of the codes that are required by the system. One of the people we talked to in the facilities said the only time he noticed problems with data accuracy were when inexperienced clerks were working in the administration office.

The Age of the Offender Management System in General, and the Movement System in Particular, Increase the Risk of System Failure

The Offender Management System was created in the late 1970s and is written in a programming language that fewer and fewer programmers are familiar with. In addition, like most programs of its age, the programming is poorly documented. As a result, when people need to fix a problem in the system, or add a new transaction code, it's difficult for programmers to know how make the needed changes. The lack of documentation also makes it difficult to predict the effects any change will have on the rest of the system.

Many parts of the Offender Management System have been updated to some extent in the years since it was created. However, the Movement system hasn't been updated. This impacts many other parts of the Offender Management System because many of the other parts of the System depend on data from the Movement system's data tables to complete their operations.

The age of the Offender Management System, the lack of documentation, and the dependence on the Movement system, significantly raise the risk of a catastrophic failure of the System. If the Movement system failed, many of the functions of the Offender Management System would also experience problems. While we found that the system had fairly good controls over data accuracy, it would be difficult to say that the system's data is "reliable" because of the risks that the age of the system pose.

Recommendations

To reduce the risk of the Department's computer systems containing inaccurate or incomplete data, the Department should do the following:

a. develop data entry controls for use in the correctional facilities, such as requiring data entry supervisors to check the accuracy of a percentage of transactions daily

b. develop training manuals and user manuals for the Movement system

c. begin planning to replace the Offender Management System with a more modern system, or update the Movement system and any other parts of the Offender Management System that are outdated. As part of that project, the Department should ensure that the new system provides for audit trail information, and allows for less confusing data entry.

Question 2: Does the Department Adequately Manage the Maintenance and Updating of Its Critical Software?

An organized approach to managing changes to important computer programs is essential to maintaining their reliability. Overall, the Department's practices in managing changes to the Total Offender Documentation System are good. Its use of user groups to approve and test changes to the System is excellent, but other parts of the change control process could benefit from being more formalized and better documented.

Because of the Dynamic Nature of Computer Software, It's Important to Have a Well Organized System To Manage the Process Of Making Changes

In many ways, software is delicate and difficult to maintain. A large and complex computer program, such as the Total Offender Documentation System, is constantly in flux. Various things in the software always need to be changed or corrected. For example, there are functions that didn't get included in the initial version of the program. There are bugs. There are changes to reflect new laws or regulations, and there are changes to increase efficiency. In addition, users frequently find things they would like to have added or altered to make the system easier to use. As a result, computer programs remain works in progress long after they are put into daily use.

If the process for altering software isn't closely organized and managed, the software can quickly become unreliable. Managing changes in software is called "change control."

Among the best practices for change control identified by COBIT are the following:

- Using a formal process, such as a change control committee, to review change requests
- Categorizing and prioritizing requested changes
- Documenting change requests in writing
- Documenting authorization of changes
- Analyzing the technical and security impact of a requested change prior to approval
- Using a formal tracking system to control changes
- Updating user manuals when changes in the program are instituted
- Involving users in the testing of the changes before they are put into production
- Requiring documented information systems management approval before changes are put into production

The Department uses different change control policies for the Total Offender Documentation System and the Offender Management System. We reviewed the Total Offender Documentation System's change control policies for this audit because it's a new system and should reflect the most up-to-date policies used by the Department.

The Department Places The Responsibility for Managing Changes On The Users, Where It Belongs.

The Total Offender Documentation System changes are approved and monitored by several steering groups–a parole steering group, and three community corrections steering groups. Issues that overlap parole and community corrections are handled by an executive committee made up of representatives from all four steering committees. These committees are made up of different types of users from across the state, as well as representatives from the Total Offender Documentation System programming staff.

When one user group recommends a change to the system, the recommendation is submitted in writing to the executive committee. The Total Offender Documentation System supervisor provides to the committee estimates of the resources necessary to make the change, then the committee decides whether or not to make the change.

If the executive committee approves a change, programmers assigned to that system do the work. The committee prioritizes the programmers' work by deciding which changes are the most important.

The Department has recently developed an online method of tracking requested changes. Users request changes on an electronic form. As the request goes through the approval process, it is updated on-line. This method allows the requestor to monitor the request's status online. The steering group that originally requested the change actively monitors the progress of the change throughout the process. This method also provides a means for Division officials to check the status of all recommended changes.

After completing a change to a program, the programmer tests it. If it's a major change, a test version of the system software is set up and users test the change. When users and the Total Offender Documentation System supervisor are satisfied with the change, the change is made in the "production" version of the software. (The production version of the software is the copy of the program that is actually doing the work.)

Overall, the Change Control Process Needs To Be Better Organized and Documented

The system of user groups the Department uses to control the process is well designed. Control of changes by users instead of the information systems staff is appropriate. Our review of minutes of the groups' meetings show that they take their responsibility seriously. Additionally, the Total Offender Documentation System programming supervisor appears to be very well organized. However, change control as a whole could be improved by adding more organization and better documentation as called for in the COBIT standards. That would ensure process continuity if the current supervisor left the agency.

We found that the Department recently began making improvements to the organization of the process. For example, online requesting and tracking of changes was being instituted at the time of the audit. This will be a great improvement over the manual process. We attempted to track a sample of changes through the process from the date they were requested to the date they were completed and found it very difficult. In addition, the new online system will provide more documentation of management approvals than the previous system did.

Additional improvements are needed, however. Specifically, the Department could improve its system by:

- Developing written change control policies. Currently, it has none.

- Developing a policy requiring the system supervisor to approve in writing incorporation of software changes into the production software. This is necessary to reduce the risk of a programmer inserting untested or poorly tested modifications into the production software. Also, this approval process would give the Department a change control log that would document each change instituted in the production software.

- In the case of significant changes, requiring formal user acceptance tests before the final changes are allowed to be incorporated into the production software. In our review of changes to the system, users were sometimes, but not always, involved in testing.

- Requiring staff to update user operation manuals when changes are made to the software. Currently, system staff notify users of changes to the system each month in an e-mail. This method is useful for change notification but makes it very difficult for a user to find the answer to a specific question about using the

system. Also, the email method makes training new staff particularly difficult because notices are not compiled into a single reference or training manual.

Recommendations

To ensure adequate management of the maintenance and updating of Total Offender Documentation System, the Department should:

a. develop written change control policies

b. develop a policy requiring the system supervisor to approve, in writing, all movements of software changes into the production software

c. require formal user acceptance tests before large programming changes are incorporated into production software

d. require updates to user operation manuals when changes are made to the software.

Question 3: Has the Department Adequately Planned For the Actions It Must Take In The Event Of A Disaster To Minimize the Loss of Computer Operations?

The Department has done little business continuity planning for its information systems. It has some important beginnings—a good system to back up and protect critical data, and a minimal disaster recovery plan. However, officials haven't done any planning to more fully prepare for the most likely types of disasters. The Department's current disaster recovery plan doesn't describe the steps staff would need to take to recover from a disaster, officials haven't made any arrangements for off-site processing, nor have officials addressed important telecommunication and security matters that might arise. Finally, staff haven't been trained in appropriate emergency procedures.

An Organization Needs Good Business Continuity Planning In Order To Quickly Recover Critical Operations After a Disaster

Over the years many different terms have been used for planning for recovery from computer outages, such as "disaster recovery," "contingency planning," and "business continuity planning." All have a slightly different focus, with business continuity planning being the most all encompassing. Business continuity planning addresses an organization's ability to continue functioning when normal operations are disrupted. By necessity, it includes planning for contingencies, and planning for disaster recovery and is focused on the information system functions that are the most necessary to continued agency operations.

According to COBIT, when an organization implements good business continuity planning, management:

- develops a written continuity plan that is in line with the organization's objectives
- reviews and updates the plan periodically
- tests the plan and periodically updates it based on the test results
- conducts periodic staff training on carrying out the plan
- establishes adequate off-site storage for critical backup tapes
- identifies alternatives for backup processing sites and replacement computers
- contracts for offsite hardware and processing facilities in advance of an emergency
- develops alternative processing procedures for user departments to implement until processing can be restored

The continuity plan itself should:

- contain an inventory of the most critical hardware, software, and supplies
- discuss the most likely types of disasters and describe various levels of disaster
- specify detailed steps to take to recover services, including assigning specific roles and responsibilities to specific staff members
- detail how to operate the critical computer programs

The Department Has Done Little Business Continuity Planning For Its Critical Computer Programs

Continuity planning enables an organization to minimize the loss of communications and important computer operations during an emergency. As agencies become increasingly dependant upon computer programs in all areas of their operations, the ability to quickly and effectively recover from adverse conditions becomes essential. This is especially true for an agency with important public safety responsibilities such as the Department of Corrections where management of offenders is highly computerized. Good continuity planning can significantly increase the probability of surviving a major disaster.

Department management has implemented some sound practices. A well developed system for backing up critical data, including off-site storage of backup tapes, is in place. The Department also has a limited continuity plan which staff reports is periodically updated. Finally, the Department has developed alternative procedures for users to follow when computer services are unavailable, although the procedures aren't written.

However, the Department doesn't meet many other COBIT standards. Shortcomings in the Department's contingency plans could result in a significant delay in resumption of normal operations after a disaster. We found the following problems:

The Department hasn't conducted a risk analysis to assess possible disaster scenarios or threats. During continuity planning, managers must identify types of disasters that are most likely to occur so that they can identify appropriate preparations in the disaster recovery plan. For example, officials may decide that a likely disaster would be a tornado. They would begin the planning process by identifying the potential impact of a severe tornado hitting the agency offices or other facilities, and necessary steps to recover operations. The risk assessment portion of the continuity plan would identify various scenarios.

The existing continuity plan doesn't assign roles and responsibilities to specific staff, and is limited in the recovery instructions it gives. Once risks have been assessed, action plans must be developed to enumerate specific steps staff would need to take to react to each likely type of disaster. These steps are recorded in the disaster recovery plan. For the plan to be effective, it also needs to assign specific steps and responsibilities to specific staff. Documentation of these steps and assignments form the core of the disaster recovery plan Few people can react efficiently in an emergency. However, if staff have planned well, when an emergency occurs staff won't have to think about what to do, they would just follow the directions in the plan.

The Department's current disaster recovery plan is a detailed instruction manual for loading backup tapes and operating a replacement computer after one has been located. However, it contains no instructions for activities required to recover operations to the point of actually being ready to operate a replacement computer. It also fails to assign responsibilities to specific staff.

The Department hasn't made any arrangements for offsite processing for its critical computer programs. Most of the Department's critical computer programs reside on the Department's mid-range computer (A mid-range computer is similar to a mainframe computer, only smaller). Department officials told us that if there was an emergency they would call the computer manufacturer and ask to borrow a replacement computer. The DISC official in charge of disaster recovery told us that many organizations take the same approach, but when a disaster occurs find that manufactures don't have large computers sitting idle. The Department needs to develop formal agreements with a company that specializes in providing computing facilities during emergencies. Department officials told us they have begun gathering information on making arrangements for alternative offsite facilities.

The current plan doesn't address telecommunications and security issues that would arise if processing had to take place at a site other than the Department's main office or one of the correctional facilities. A great deal of confidential information is transmitted over the Department's network when data are sent from correctional facilities to the central office. If something happened to the offices in the Landon building, it is likely that the Department would have to use a computer at another site. However, no planning has been done to think about how to secure transmission from the correctional facilities to a computer in a new location.

The Department has no training for staff in what to do in an emergency. This is crucial because emergencies are chaotic by definition. A good plan assigns specific responsibilities to specific staff people. Without training, when an emergency occurs staff are disorganized and it takes much longer to recover processing.

The Department Is Not In Compliance with Information Technology Executive Council Policy on Business Contingency Planning

The Information Technology Executive Council is responsible for adopting information technology policies and procedures for all state agencies. The Council has a policy on contingency planning (Policy 3210) that's very similar to the COBIT standards. In addition, the policy requires agencies to file a copy of their continuity plans with the Chief Information Technology Officer of the Executive Branch for review, and another copy with the Division of Information Systems and Communication for archiving. The Department hasn't complied with that policy.

Recommendations

1. To ensure that it reacts optimally in the event of a disaster, the Department should modify its 1. business continuity planning to include the following:

   a. a risk analysis that assess the most likely disaster scenarios

   b. an expanded disaster recovery plan that addresses the most likely disasters that might befall the Department. This plan should assign roles and responsibilities to specific staff, and present specific steps for the staff to follow in recovering computer operations. It should also address the telecommunications and security issues that would arise if the Department had to conduct computer operations off site

   c. arrangements with a vendor or contractor for the use of a computer suitable for operating the Department's critical computer programs and applications during emergencies

   d. training staff in how to use the plan in the event of an emergency.

2. The Department should bring itself into compliance with the requirements of the Information Technology Executive Council's policy on contingency planning.

APPENDIX A

Agency Response

On November 15, 2001, we provided copies of the draft audit report to the Department of Corrections. Its response is included in this Appendix.

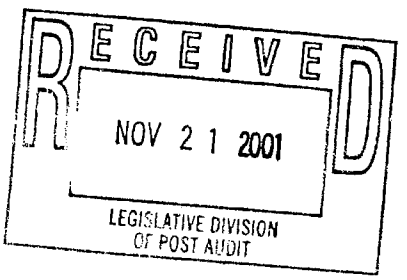
STATE OF KANSAS

DEPARTMENT OF CORRECTIONS
OFFICE OF THE SECRETARY
Landon State Office Building
900 S.W. Jackson — Suite 400-N
Topeka, Kansas 66612-1284
(785) 296-3317

raves
rnor

Charles E. Simmons
Secretary

November 21, 2001



Ms. Barbara Hinton, Legislative Post Auditor
Legislative Division of Post Audit, Mercantile Bank Tower
800 SW Jackson Street Suite 1200
Topeka, Kansas 66612-2212

Dear Ms. Hinton:

I have reviewed the draft audit report, *Department of Corrections: Reviewing the Adequacy of Its Controls Over Its Information Technology Systems*, and would like to offer the following comments in response.

In general, I concur with the report's basic findings and recommendations. The department has identified improvement of its management information systems as a major operational priority and has reflected this priority in a recently prepared issue paper, in the department's updated Strategic Action Plan, and in the FY 2003 budget request.

Before responding to specific recommendations in the audit report, I would like to provide background information on some of the department's recent activities in this area.

Last spring I directed that an issue paper be developed on the status of the department's offender-based management information systems. The purpose was to identify problems and limitations which may exist, to identify options for addressing short-term and long-term problems, and to emphasize the importance of MIS improvements on data quality and public safety. A KDOC working group was established to examine MIS issues and while the scope of our internal review was not exactly the same as the scope of the audit prepared by your staff (our review did not include contingency planning, for example), there is much similarity between the findings reached in the two reports. In the department's report, five major issues were addressed. For each issue, the task

group defined the problem, suggested a goal, and identified options and recommendations. Many of the task group's recommendations mirror those in the audit report, such as the need to:

- modernize the Offender Management Information System, integrate it with other departmental MIS applications, improve its user friendliness and accessibility of its data;
- provide training and reference manuals for MIS users; and,
- improve data quality.

Attached is a copy of the summary of the issue paper. The complete report is available upon request.

Last summer the department also issued its updated three-year Strategic Action Plan. One of the plan's six major goals is to "manage accurate, timely and complete information." Three of the objectives supporting this goal relate directly to the audit report findings. These objectives are:

> By June 2003 data quality assessment tools for critical OMIS and TOADS systems will be identified, be under development or be implemented.
>
> By June 2004 fifty percent of offender information will be in a user-friendly format.
>
> By June 2003 a comprehensive IT training program will be developed throughout the department.

The biggest obstacle we face in making the MIS improvements identified in the issue paper, the strategic plan and the draft audit report is the lack of adequate resources. The task group's issue paper estimated an additional annual budget need of $2.4 million and 43 FTE to fully implement its recommendations. The group proposed a phased implementation, with first-year funding of $1.2 million and 23 positions. The department included the first phase as a high priority item in its FY 2003 enhanced services level budget request, but given the state's current fiscal condition, it is unknown when resources might be available for this type of initiative.

The department has utilized and will continue to explore opportunities for federal grant funds to support development and improvement of MIS systems. Recent examples include the use of Byrne and National Governors' Association grant funds for TOADS and CJIS (Criminal Justice Information System) related projects. We also plan to include an information technology component in future grant applications and contracts. However, funding available through these sources is targeted for specific purposes and, while we attempt to expend them in a manner consistent with our overall MIS objectives, there are limitations as to how they may be used.

As indicated in the comments below regarding the audit report's specific recommendations, we have plans to begin addressing many of them. However, it should also be understood that, given existing levels of staff and funding, we are quite limited in how much we can do and how quickly. Without additional resources, even high priority projects may require a protracted timetable or be implemented only partially.

Question 1: Has the Department Developed Adequate Policies to Ensure That Data in Its Computer Systems Are Entered Accurately and Completely, and Reliably Maintained?

To reduce the risk of the Department's computer systems containing inaccurate or incomplete data, the Department should do the following:

a. ***Develop data entry controls for use in the correctional facilities, such as requiring data entry supervisors to check the accuracy of a percentage of transactions daily.***

Controls exist in some of the Offender Management Information Systems and Total Offender Activity Documentation System applications. They are designed as data validity checks to prevent inappropriate responses such as entering text when numeric data is required, etc. The need to improve data quality, however, is recognized both in the department's MIS issue paper and strategic plan.

Guarding against improper data entry requires the efforts of both users and managers. The users must take due care in ensuring that the right information is being entered into the system at all times. Training can help correct errors which are made consistently. Random errors can be reduced by the user inspecting the entered information before it is accepted by the system. These two areas will be addressed in future training being developed for the offender systems. Supervisors and managers at all levels must be willing to use existing reports and data screens to analyze data and to identify errors in data entry. Development of this management practice will be stressed in future information systems training curricula.

b. ***Develop training manuals and user manuals for the Movement system:***

- The need for training and development of user manuals is recognized in the department's MIS issue paper and strategic action plan.

- A user manual committee is being convened to develop a comprehensive user manual for the Offender Management Information System (which includes Movement, as well as other major subsystems). With existing resource levels, this

effort will likely be a prolonged project. Users from throughout the system will participate.

- The Total Offender Activity Documentation System (TOADS) user and training manuals are constantly being updated to reflect the newest features and enhancements.

- All new systems will require the creation and development of user manuals as part of the deployment phase.

- Vendors will be required to deliver user manuals as part of any new information system projects.

c. ***Begin planning to replace the Offender Management (Information) System with a more modern system, or update the Movement system and any other parts of the Offender Management (Information) System that are out-dated. As part of that project, the Department should ensure that the new system provides for audit trail information, and allows for less confusing data entry.***

The requirement to replace or upgrade OMIS has long been a recognized need for the department, and is one of the major topics addressed in the MIS issue paper.

The following initiatives are underway to address movement data issues and MIS system modernization and integration:

- A Movement Data Re-engineering Committee will be organized in calendar year 2002 to identify the scope of the problem and to develop a structure that will improve movement data access and utility.

- The department supports two Strategic Action Plan objectives that relate to improving the quality and accessibility of data and developing user-friendly approaches to retrieving and using data.

- The department will continue to seek ways to create and staff a full development team to focus on improving data accessibility and data structures.

Question 2: Does the Department Adequately Manage the Maintenance and Updating of Its Critical Software?

To ensure adequate management of the maintenance and updating of Total Offender Documentation System, the Department should:

a. ***Develop written change control policies.***

Change control is practiced at the operational level through the use of various natural work groups. Written policies will be developed and documented in the department's Internal Management Policies and Procedures (IMPP). The next scheduled review and revision of information system IMPP's will occur in January 2002.

b. ***Develop a policy requiring the system supervisor to approve, in writing, all movements of software changes into the production software.***

This policy is now in effect and will be codified in the IMPP's after the January 2002 reviews. The Applications Development / Support Section will review and evaluate software that enforces change control management techniques to include supervisor approval of code modifications.

c. ***Require formal user acceptance tests before large programming changes are incorporated into production software.***

User acceptance is part of application development testing and evaluation. Currently, no clearly defined procedures are in place, however. One of the obstacles to more structured user acceptance testing is the availability of operational staff to participate in the tests. Future IMPP revisions will address a more formal methodology of achieving user acceptance.

d. ***Require updates to user operation manuals when changes are made to the software.***

The Total Offender Activity Documentation System (TOADS) manual is routinely reviewed by both the Parole Steering Group and the TOADS Users Group. We have also begun efforts to develop a comprehensive Offender Management Information System (OMIS) manual. Once the manual is developed, procedures will be implemented that require the review of the manual on a routine basis and after major OMIS revisions.

Question 3. Has the Department Adequately Planned for the Actions IT Must Take In the Event Of A Disaster to Minimize the Loss of Computer Operations?

1. **To ensure that it reacts optimally in the event of a disaster, the Department should modify its business continuity planning to include the following:**

a. ***A risk analysis that assess the most likely disaster scenarios.***

We will begin the risk analysis in January 2002. We are in the early stages of identifying a methodology to assess risks. The risk analysis conducted for the Y2K contingency will be a foundation for the updated assessments.

b. ***An expanded disaster recovery plan that addresses the most likely disasters that might befall the Department. This plan should assign roles and responsibilities to specific staff, and present specific steps for the staff to follow in recovering computer operations. It should also address the telecommunications and security issues that would arise if the Department had to conduct computer operations off site.***

The department currently has a disaster recovery plan for the main offender systems. We are lacking plans for all systems, however. This will be a significant project and development of comprehensive plans will take months to complete. There is a framework in the Y2K plans. These must be updated to reflect the new systems and incorporate more detailed responses.

c. ***Arrangements with a vendor or contractor for the use of a computer suitable for operating the Department's critical computer programs and applications during emergencies.***

We have evaluated several options to outsource the hardware contingency aspects of the plan. The fact that the department has several critical systems means that available options are both costly and complex. No funding is currently available for this purpose.

The department is considering hosting a separate off-site facility that will serve as a backup site for the major central office and facility systems. In the interim we are distributing systems to several facilities to minimize the impact of a local disaster on all of the critical systems. Implementing this recommendation will be costly regardless of who owns or hosts the hardware.

d. ***Training staff in how to use the plan in the event of an emergency.***

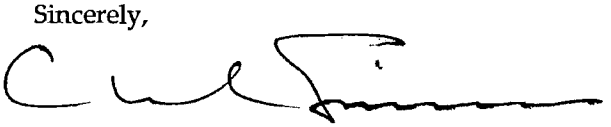
Once the contingency plans for each facility and major office have been developed, key leaders, IT staff and local staff will be trained on the major components of the plans. Actual testing of the plans will require dependence on DISC for networking support and any evaluation of the plans.

2. **The Department should bring itself into compliance with the requirements of the Information Technology Executive Council's policy on contingency planning.**

Policies are being developed that will place the department's contingency practices in compliance with ITEC.

I hope this provides you with the information requested. Please let me know if you have questions or require additional information.

Sincerely,



Charles E. Simmons
Secretary

Attachment