



**New Jersey State Legislature
Office of Legislative Services
Office of the State Auditor**

**Department of the Treasury
Division of Revenue
Information Systems**

July 31, 2002 to June 27, 2003

**Richard L. Fair
State Auditor**

LEGISLATIVE SERVICES COMMISSION

SENATOR JOHN O. BENNETT
Co-Chairman

SENATOR RICHARD J. CODEY
Co-Chairman



ASSEMBLYMAN ALBIO SIRES
Vice-Chairman

SENATE

BYRON M. BAER
ANTHONY R. BUCCO
NIA H. GILL
BERNARD F. KENNY, JR.
ROBERT E. LITTELL
ROBERT W. SINGER

GENERAL ASSEMBLY

PETER J. BIONDI
FRANCIS J. BLEE
ALEX DECROCE
PAUL DIGAETANO
JOSEPH V. DORIA, JR.
JOSEPH J. ROBERTS, JR.
LORETTA WEINBERG

New Jersey State Legislature

OFFICE OF LEGISLATIVE SERVICES

OFFICE OF THE STATE AUDITOR

125 SOUTH WARREN STREET
PO BOX 067
TRENTON NJ 08625-0067

RICHARD L. FAIR
State Auditor
(609) 292-3700
FAX (609) 633-0834

ALBERT PORRONI
Executive Director
(609) 292-4625

The Honorable James E. McGreevey
Governor of New Jersey

The Honorable John O. Bennett
President of the Senate

The Honorable Richard J. Codey
President of the Senate

The Honorable Albio Sires
Speaker of the General Assembly

Mr. Albert Porroni
Executive Director
Office of Legislative Services

Enclosed is our report on the audit of the Department of the Treasury, Division of Revenue Information Systems for the period July 31, 2002 to June 27, 2003. If you would like a personal briefing, please call me at (609) 292-3700.

A handwritten signature in black ink, appearing to read "Richard L. Fair".

Richard L. Fair
State Auditor

August 28, 2003

Table of Contents

	Page
Scope	1
Objectives	1
Methodology	1
Conclusions	2
Findings and Recommendations	
Business Continuity and Disaster Recovery	3
Computer Room Security	4
Transfer of Image Platters	5
System Documentation/Change Management	6

**Department of the Treasury
Division of Revenue
Information Systems**

Scope

We have completed an audit of the Department of the Treasury, Division of Revenue Information Systems for the period July 31, 2002 through June 27, 2003. Our audit evaluated selected application and general controls related to the processing of documents and recording of data through the DP500 remittance processor, Document Processing System (DPS), and the Data Capture and Retrieval (DCR) system. Our tests of general and application controls were limited to those in place for transaction processing data integrity, data security, backup and recovery, and contingency planning and disaster recovery.

The prime responsibility of the Department of the Treasury, Division of Revenue is to accurately and efficiently provide data and revenue processing, image and electronic archival storage, and registration and recording services, as well as to enhance revenue through bad debt collection for all of their clients.

Objectives

The objectives of the audit were to determine the adequacy of selected application and general controls. These controls include policies and procedures to provide system management and continuity, ensure transaction processing data integrity, and provide data security.

This audit was conducted pursuant to the State Auditor's responsibilities as set forth in Article VII, Section 1, Paragraph 6 of the State Constitution and Title 52 of the New Jersey Statutes.

Methodology

Our audit was conducted in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. Additional guidance for the conduct of the audit was provided by *Federal Information System Controls*

Audit Manual issued by the United States General Accounting Office and *Control Objectives for Information and related Technology* issued by the Information System Audit and Control Foundation.

In preparation for our testing, we studied legislation, administrative code, circular letters promulgated by the State Comptroller, and policies of the division. Provisions that we considered significant were documented and compliance with those requirements was verified by interview, observation, and through our samples of transactions. We also interviewed division personnel to obtain an understanding of the programs and the internal controls.

A nonstatistical sampling approach was used. Our tests of application and general controls were designed to provide conclusions about the adequacy of those controls in place for transaction processing data integrity, data security, backup and recovery, and contingency planning and disaster recovery. Sample transactions were judgmentally selected for testing.

Conclusions

Our review disclosed that while selected application controls were in place and functioning adequately for transaction processing data integrity, the selected general controls for system management and continuity, and for data security were not adequate.

We have also provided the Department of the Treasury with a management letter containing a more detailed discussion of one of the computer control weaknesses.

Business Continuity and Disaster Recovery

**The division's
disaster recovery
capabilities are not
adequate.**

The division processes revenue and the related documentation for many state agencies. The capability to process this revenue and data is important to state operations. Therefore, procedures must be in effect to safeguard information resources, minimize the risk of unplanned interruptions, and enable the recovery of critical operations in the event such interruptions occur. This comprehensive business continuity plan should address all potential disruptions to division operations.

Recommendation

We found the division's disaster recovery plan and capabilities to be inadequate, and we have provided the department and division with further technical detail to allow them to address these issues.

Auditee's Response

In the event of a disaster, the state's inability to process incoming revenues would have a dramatic effect on the state's fiscal stability. In addition, inconveniences to the public would occur because of the state's failure to issue income tax refunds; property tax rebates; driver license and motor vehicle registration renewals; and professional license renewals. Delays in processing the data required to issue unemployment and disability payments would occur. The division has prepared a space planning request (SPR) that addresses space needs for the entire division. As part of that SPR, disaster recovery problems are identified and suggested solutions are offered. In addition, the division has recently completed its Business Continuity Plan that identifies, in detail, contingency plans in the event of a disaster. This Business Continuity Plan was part of the department's overall strategy for increasing emergency preparedness throughout the department.



Computer Room Security

Access to the
Adivision's
computer room facility
should be secured and
monitored.

The computer room houses the division's servers, FileNET jukeboxes, other forms of hardware, and the original and backup image platters. The door does not contain a locking mechanism allowing access by all personnel to the premises. In addition, access to the room is not adequately monitored. The lack of security over access to the computer room facility jeopardizes the division's hardware and image platters stored in the room. The potential risk of loss to the equipment and essential data would result in the division's inability to run mission critical applications.

Recommendation

The division should install a locking mechanism on the door allowing monitored access only to authorized personnel.

Auditee's Response

The Division of Revenue's Processing Center at Mill Hill is a secure facility requiring key-card access to enter the building. Authorized employees (both Technical and Operational) are in and out of the room all day to perform the routines their jobs require. After the last employee leaves from second shift the building is secured by the State Guards, the alarms are set, and the doors are locked.

That being said, we realize that there is an exposure for unauthorized employees to enter the computer room and intentionally or unintentionally create problems. Immediately after preliminary discussion with the on-site State Auditors, the division secured funding and submitted a Tenants Service Request to restrict access to the computer room either by using keycards or some other approved security method (i.e., pin number lock).



Transfer of Image Platters

Backup image platters should be stored separately from the originals.

The original revenue documents are scanned and the resultant images are stored on platters. If these platters were lost or damaged the division and their clients would be unable to retrieve the document images. Significant time and cost would be required if lost images needed to be recaptured. Backup platters are first stored in the same unsecured location as the original platters of images until they are later transferred off-site. No schedule is maintained to relocate the backup platters off-site on a periodic basis; the last transfer of backup platters was April 17, 2003. All backup sources of information need to be separated from the original according to a predetermined schedule to safeguard and protect the information against possible loss.

Recommendation

The division should store all backup platters separately from the originals upon creation. The division then needs to establish a procedure that relocates the backup image platters to an off-site storage facility on a scheduled basis to ensure that the backup and recovery of images can be maintained.

Auditee's Response

In the business process of committing (burning) images to optical disk, a second platter is created (translog) for backups and disaster recovery. These translogs are accumulated and sent to the Division of Archive Management (DARM) for storage (and retrieval if needed). The audit exception states that the translogs are stored in the same unsecured location as the image platters and there is no schedule for sending the translogs to DARM. As noted in the previous section, computer room security will be improved. In addition, the Image Analyst in Technology Services is now boxing and sending the translog platters to DARM every Friday as a regularly scheduled delivery.



System Documentation/Change Management

The available current documentation does not provide a sufficient basis for effective system development and maintenance.

We noted a lack of documentation for the Document Processing System (DPS) and the Data Capture and Retrieval (DCR) system. An understanding of a system's functionality and operational relationships is impaired by the lack of sufficient system documentation. This understanding is further impaired by the division's failure to require system documentation to be periodically updated to reflect all changes made to the processing functions.

Developing and maintaining adequate documentation for the DPS and DCR systems will enable the division to reconstruct and resume operations at the current level in the event of unexpected system failure. It also minimizes the likelihood of disruption, unauthorized alterations, and errors during system modifications.

Recommendation

The division should require the development and maintenance of adequate system documentation identifying the current status of operations. In addition, each change needs to be incorporated into the documentation to provide information on the present conditions of the systems.

Auditee's Response

The Division of Revenue's Technology Services Branch has neglected documentation as the Auditors found.

In 2002, Technology Services received authorization to hire an additional two full-time analysts for system responsibilities. In addition, authorization was granted for the use of Intermittent Technicians to supplement our response to day-to-day system problems. The use of Intermittent Technicians to resolve routine problems has allowed us to assign the two new analysts full-time to both the Document Processing System (DPS) and the manual data entry system (DCR). In 2003, funding approval for the

upgrade of the DCR system from old unsupported hardware and software to a current state of the art hardware and software platform was received. This process began in the spring and will be completed this fall. As a result of the new system and a full-time analyst, we expect that all DCR documentation will be up to date by the end of 2004, and as a full-time analyst is now assigned that documentation and changes will be integrated as a matter of routine in the future.

DPS will go through a relatively major upgrade of its operating system and core processing software this summer. As a result, all DPS documentation will be updated and current by the middle of January 2004. The reason for this later date is all of our processing software will again be updated for the 2004 tax season (tax year 2003) in January. This will result in the most up-to-date documentation, and as a full-time analyst is now assigned to DPS, documentation will be updated and changes will be integrated into the documentation as a matter of standard operating procedure.

