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

Office of Information Technology
Data Center Operations and Production Controls

September 1, 2010 to June 22, 2011

Stephen M. Eells
State Auditor

New Jersey State Legislature

OFFICE OF LEGISLATIVE SERVICES
OFFICE OF THE STATE AUDITOR
125 SOUTH WARREN STREET
PO BOX 067
TRENTON NJ 08625-0067

ALBERT PORRONI
Executive Director
(609) 292-4625

OFFICE OF THE STATE AUDITOR
(609) 292-3700
FAX (609) 633-0834

STEPHEN M. EELLS
State Auditor

THOMAS R. MESEROLL
Assistant State Auditor

JOHN J. TERMYNA
Assistant State Auditor

The Honorable Chris Christie
Governor of New Jersey

The Honorable Stephen M. Sweeney
President of the Senate

The Honorable Sheila Y. Oliver
Speaker of the General Assembly

Mr. Albert Porroni
Executive Director
Office of Legislative Services

Enclosed is our report on the audit of the Office of Information Technology, Data Center Operations and Production Controls for the period of September 1, 2010 to June 22, 2011. If you would like a personal briefing, please call me at (609) 292-3700.

Stephen M. Eells
State Auditor
September 1, 2011

Table of Contents

Scope

We have completed an audit of the Office of Information Technology (OIT), Data Center Operations and Production Controls for the period September 1, 2010 through June 22, 2011. Our audit evaluated selected general controls in place over operations and production for the IBM z/OS mainframe operating system. We reviewed only the mainframe partition that contains various applications for the Department of the Treasury. Our scope did not include any other mainframe partitions that run applications for other state departments, and it did not include any data storage peripherals. The operations controls reviewed are part of the system software for z/OS. System software refers to the files and programs that make up the computer's operating system, and is designed to operate the computer hardware by providing and maintaining a platform for running application software. The production controls are those associated with change management of the revisions to z/OS. The purpose of change management is to effectively manage changes for all operating systems in order to maintain data integrity, system availability, and system stability, and to increase the level of service provided by OIT to the client community

The state maintains two data center facilities known as the HUB and River Road data centers. The HUB data center houses the Bull mainframe computer and client servers, as well as providing state printing processes. The River Road data center contains the IBM mainframe computers and the server farm for clients. It also includes the Network Control Center and the System Control Center, which is the help desk for all state departments. Both facilities process various mission critical applications for the state. Each facility is integral in the processing of applications that are vital to the functioning of the state and for providing electronic services to its citizens.

Objectives

The objective of the audit was to determine the adequacy of selected general controls over the platform which supports the major applications the state relies upon. These controls included policies, standards, and procedures to properly operate, maintain, and safeguard the IBM z/OS operating system.

This audit was conducted pursuant to the State Auditor's responsibilities as set forth in Article VII, Section I, 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 conduct of the audit was provided by *Control Objectives for Information and related Technology* (CobiT) issued by the IT Governance Institute and the *Federal Information System Controls Audit Manual* (FISCAM) issued by the United States Government Accountability Office (GAO).

In preparation for our testing, we studied circular letters promulgated by the Department of the Treasury, and policies and guidelines of the agency. Provisions that we considered significant were documented, and compliance with those requirements was verified. In addition, we obtained and reviewed documentation and procedures pertaining to internal controls over system software and change management. Functions we considered significant were documented and implementation of those features was verified. We also interviewed agency personnel to obtain an understanding of the internal controls.

A nonstatistical sampling approach was used. Our tests of general controls were designed to provide conclusions about the adequacy of those controls in place for system software and change management.

Conclusions

While OIT staff has established appropriate general controls over system software and change management, our review disclosed that improvement is needed to ensure that these controls are adhered to and regularly updated.

System Software Documentation

Documentation for the IBM z/OS needs to be formalized to illustrate the current configuration of the operating system.

In accordance with control objectives provided by *Control Objectives for Information and related Technology* (CobiT), knowledge about changes made to application hardware and software should be documented in a timely manner. The time lapse between changes being made and the documentation reflecting those changes should be kept to a minimum to ensure that the documentation is complete and correct. OIT's Technical Services – Systems Support and Integrity staff has informal documentation that does not present an accurate picture of how the operating system is currently configured. Accurate documentation for the current configuration of the IBM z/OS would provide knowledge capture and sharing for current and future staff by minimizing the exposure to critical dependency on key individuals who are nearing retirement age. Due to limited staff resources, updating documentation does not receive priority amongst the many responsibilities that demand the staff's time.

Recommendation

The Technical Services – Systems Support and Integrity staff should formalize the documentation of the z/OS to adequately reflect the current configuration of the operating system. OIT also needs to address the staffing issues that will be affected by the retirement of key personnel in the foreseeable future. Without formalized documentation, the probable reduction in staff may result in vulnerability in this area.

»➤◅«

Operating System Monitoring

The z/OS operating system should be actively monitored to ensure its intended configuration, efficient performance, and utilization of only current versions of software.

In accordance with *Federal Information System Controls Audit Manual*, current configuration information should be routinely monitored for accuracy. Monitoring should address the current baseline and operational configuration of the hardware, software, and firmware that comprise the information system. Information technology products should be configured in compliance with industry standards and the vendors' recommended security practices. The entity should have the capability to monitor and test that software is functioning as intended. The present configuration of the IBM z/OS operating system contains libraries, programs, and files that are obsolete, unused, and even unknown. This could lead to an unintended vulnerability and exposure. Regular monitoring would identify system, application, and security exposures in the z/OS reducing the potential risk to the operating system and the applications processed by the operating system. The Technical Services – Systems Support and Integrity staff have limited personnel available to install and maintain the z/OS operating system. This restricts their ability to monitor z/OS on a regular basis unless a problem arises.

Recommendation

The Technical Services – Systems Support and Integrity staff have a monitoring tool available to them known as CA Auditor. This product helps identify system, application, and security exposures in z/OS environments. It will identify exposures resulting from improper system configuration and operational errors, as well as intentional circumvention of controls and attacks. As part of an overall program of security and software management, it is highly effective at helping to assure the integrity of the base operating system and application processing environments. The staff should be afforded the ability to use this product on a regular basis to ensure the integrity of the operating system is maintained.

State of New Jersey

CHRIS CHRISTIE
Governor

KIM GUADAGNO
Lt. Governor

Office of Information Technology
P.O. Box 212
Trenton, New Jersey 08625-0212

August 31, 2011

Stephen Eells
State Auditor
Office of Legislative Services
Office of the State Auditor
PO Box 067
Trenton, NJ 08625-0067

Re: OIT Data Center Operations and Production Controls Audit

Dear Mr. Eells:

With regard to your audit report recommendations on the Data Center Operations and Production Controls at OIT, we would like to provide the following comments:

The System Software Documentation recommendation specifically states,

"The Technical Services-System Support and Integrity staff should formalize the documentation of the z/OS to adequately reflect the current configuration of the operating system. OIT also needs to address the staffing issues that will be affected by the retirement of key personnel in the foreseeable future. Without formalized documentation, the probable reduction in staff may result in vulnerability in this area."

In an effort to formalize documentation of the z/OS to reflect the current configuration of the operating system OIT will include, in the various coding, any comments containing instructions for the timely discharge of Change Control procedure. In addition, any technical area needing further explanation due to its peculiarity to the OIT system will need to be documented. A knowledgeable party can then use his or her technical experience to complete work assignments using these additional instructions. These additions would contain the information that someone outside the system would not normally know. As a result timely documented knowledge would prevent the critical dependency on key experienced individuals who may soon retire.

The Operating System Monitoring recommendation specifically states,

"The Technical Services-System Support and Integrity staff have a monitoring tool available to them known as CA Auditor. This product helps identify system, application and security exposures in z/OS environments. It will identify exposures resulting from improper system configuration and operational errors, as well as intentional circumvention of controls and attacks. As part of an overall program of security and software management, it is highly effective at helping to assure the integrity of the base operating system and application processing environments. The staff should be afforded the ability to use this product on a regular basis to ensure the integrity of the operating system is maintained."

There are two areas addressed in this recommendation. First identify exposures resulting from improper system configurations and operational errors. Second identify intentional circumvention of system controls and attacks.

The former involves organization of operating system libraries, programs and files. The Technical Services-System Support and Integrity staff, subject to manpower availability, can routinely utilize CA Auditor monitoring to keep system configurations current hopefully preventing operational errors. The latter area involves identification of intentional circumvention of controls and attacks. The Internal Monitoring, Audit and Controls Unit, subject to manpower availability, can routinely use CA Auditor monitoring as a circumvention of controls and attack deterrent. In either instance a frequency schedule can be established for routine proactive monitoring.

We at OIT appreciate the cooperative manner in which you and your staff conducted this audit. Your recommendations are well accepted as OIT is committed toward continual improvement. If you have any further comments, please contact our IT Audit contact Stephen Foundos at 609-633-8791. He will be available to expedite any communications throughout OIT.

Sincerely,

Gloria J. Broeker
Executive IT Management

c: D. Gerard
S. Foundos
H. Hottmann