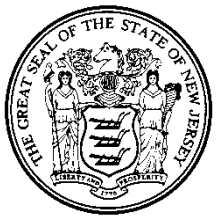

New Jersey State Legislature
Office of Legislative Services
Office of the State Auditor

Statewide Information Technology Contingency Planning

March 9, 2015 to June 10, 2016

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

PERI A. HOROWITZ
Executive Director
(609) 847-3901

OFFICE OF THE STATE AUDITOR
(609) 847-3470
FAX (609) 633-0834

STEPHEN M. EELLS
State Auditor

DAVID J. KASCHAK
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 Vincent Prieto
Speaker of the General Assembly

Ms. Peri A. Horowitz
Executive Director
Office of Legislative Services

Enclosed is our report on the audit of the Statewide Information Technology, Contingency Planning for the period of March 9, 2015 to June 10, 2016. If you would like a personal briefing, please call me at (609) 847-3470.

Stephen M. Eells
State Auditor
December 14, 2016

Table of Contents

Scope

We have completed an audit of Statewide Information Technology Contingency Planning for the period March 9, 2015 to June 10, 2016. We reviewed Information Technology (IT) contingency planning, including risk assessment and prevention, by the Office of Information Technology and by executive branch departments, agencies, and commissions.

Objectives

The objectives of our audit were to determine the adequacy of general controls for contingency planning for the state's IT systems. 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. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Additional guidance for the conduct of the audit was provided by *COBIT* issued by ISACA, the *Federal Information System Controls Audit Manual* (FISCAM) issued by the United States Government Accountability Office, and standards issued by the International Organization for Standardization.

In preparation for our testing, we studied legislation, circular letters promulgated by the Department of the Treasury and by the Office of Information Technology (OIT), and policies of the OIT. Provisions we considered significant were documented and compliance with those requirements was verified by interview, observation, and through our testing.

A non-statistical sampling approach was used. We judgmentally selected 24 state agencies representing the various IT platforms and contingency scenarios in the executive branch, and our tests of selected general controls were designed to provide conclusions about the adequacy of those controls in place for contingency planning.

Conclusions

Although the OIT and agencies' chief information officers have recognized the importance of contingency planning and have incorporated certain procedures to enable planning and recovery, the overall status of contingency planning, including risk assessment and prevention, for critical applications in the state needs improvement as a risk of failure to recover critical applications in a timely and effective manner exists. We also noted opportunities for improved

guidance and monitoring of statewide efforts.

Background

The OIT has the statutory responsibility for "providing and maintaining the information technology infrastructure of the Executive Branch of State Government, including all ancillary departments and agencies of the Executive Branch of State Government." Contingency planning is a component of maintaining the information technology infrastructure.

The National Institute of Standards and Technology (NIST) refers to contingency planning as "interim measures to recover information system services after a disruption." Almost all significant functions the state agencies perform are dependent on an information system for successful completion. If a disruption to an information system occurs, a contingency plan needs to be in place and ready to execute for the agency to resume its functions. Other common terms used for contingency plans include continuity of operations plans and disaster recovery plans.

Historically, the OIT has taken certain steps to meet its statutory responsibility in relation to contingency planning. They developed the OIT Availability and Recovery Site (OARS), located separately from existing OIT production facilities, for the purpose of providing the capability to recover critical state systems in the event of a disruption and have established the ability to recover critical mainframe applications. However, the ability to recover critical distributed computer applications at OARS has not been fully developed. Additionally, the OIT issued Policy 14-31 in October 2014 which outlined the agencies' responsibilities for recovery readiness; however, this policy does not include responsibilities for the OIT.

To determine state agencies' current level of compliance with OIT Policy 14-31, we surveyed and interviewed executive branch agencies regarding their contingency plans and testing. We found significant weaknesses which are detailed in our audit findings.

Centralized Coordination of Contingency Planning

There is no centralized monitoring or coordination of statewide contingency planning.

The OIT Availability and Recovery Site (OARS) was originally funded by appropriation acts to provide recovery capabilities for critical state applications in case of disruptions of service. OARS currently does not have the infrastructure or network capacity to provide disaster recovery for all of New Jersey's server applications defined as mission-critical by the owning agency. However, the OIT has made all state agencies responsible for their contingency planning and recovery efforts. In 2014, the OIT issued Policy 14-31 which states the agencies are to develop, maintain, and test a contingency plan for a given critical system identified in a Business Impact Analysis (BIA). The contingency plan is to describe the process for assuring the agency's ability to continue the critical business services and operations of each agency system, including systems used by branch or remote offices. These state agencies are aggressively seeking alternatives to provide recovery capability for their mission-critical server applications.

The state agencies we surveyed have many different recovery solutions employed, both in-house and with outside vendors. Results from the 24 state agencies surveyed disclosed: nine either have, or are in the process of developing, disaster recovery sites at satellite locations; three use the OIT's SAC data center; three are using the Department of Law and Public Safety server room in Hamilton; three have employed private vendors; one is using the OIT's HUB production data center; two do not have a solution; and three are using the OIT's OARS.

There is no centralized coordination of the different solutions employed by the agencies which precludes opportunities for possible cost efficiencies and the comprehensive coordination of recovery capacity between the OARS and other solutions. The OIT did not have a readily available listing of what applications are backed up and recoverable at the OARS and other locations when asked, although one was subsequently provided. The lack of centralized monitoring can also contribute to deficiencies in contingency planning and recovery readiness.

Recommendation

The OIT management should develop a methodology for monitoring and coordinating the contingency planning and recovery efforts of the executive branch. This should include regular input from all applicable agencies and policies and procedures that will require the necessary follow-up, monitoring, and support in testing the solutions.

Agencies' Contingency Solutions

Agencies' efforts to comply with the OIT's Contingency Planning Policy are varied in cost and quality.

We conducted a walkthrough of the 24 sampled state agencies' production server rooms for our contingency planning review. From our tours of these server rooms, we found the following problems. (The items that show less than 24 agencies surveyed are because the standard under review was not applicable to all agencies.)

- *7 of 24* agencies surveyed did not have proper fire suppression. These agencies have water sprinklers for fire suppression. If deployed, the water sprinklers will ruin all production server room equipment which many departments share with other departments for disaster recovery efforts.

- *12 of 23* did not maintain logs of individuals accessing their server rooms.

- *12 of 24* did not have water detectors employed to alert for water leaks or a flood.

- *8 of 24* had plumbing lines in their server rooms, and one production server room had a ladies room in the server room.

- *7 of 24* did not have smoke detectors located both on the ceiling and below the raised server room floor.

- *2 of 8* did not keep their server room access codes protected and changed regularly.

- *3 of 24* did not have redundancy with their uninterruptible power supply (UPS).

- *2 of 24* did not have proper humidity and temperature controls.

- *2 of 24* did not have their environmental controls tested annually.

All of these issues represent weaknesses per the *Federal Information Systems Control Audit Manual* (FISCAM*)* requirements for server rooms. A lack of funding for equipment and a failure to institute proper policies and procedures were the reasons cited by the agencies for these weaknesses.

Recommendation

Agencies which lack proper fire suppression, water detectors, smoke detectors, UPS redundancy, or proper humidity or temperature controls should work with the OIT to find the most cost-effective solutions. Otherwise, they risk total loss of production server room

equipment. Agencies which lack computer room access logs or who do not change their server room access codes on a regular basis, need to promulgate policies instituting these controls to prevent unauthorized access.

➳➤➶➻

OIT Availability and Recovery Site (OARS)

The OARS has operational deficiencies.

Private Ring Redundancy

The private ring, a fiber path interconnecting the HUB, River Road, and Hamilton data centers, does not have redundancy in the event of a disruption. The private ring supports inter-data center communication, SAN replication, and backup services.

The National Institute of Standards and Technology (NIST) Special Publication 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*, addresses the impact level of the availability security objective of information systems. Strategies for high-impact information systems should consider high-availability and redundancy options in their design. Options may include fully redundant load balanced systems at alternate sites, data mirroring, and offsite database replication.

Lack of redundancy with the OIT's private ring could disrupt inter-data center communications, SAN replication, and backup services for mission-critical mainframe and server applications.

Power Distribution Units

The OIT Availability and Recovery Site (OARS) is nearing its maximum power capacity. There is a single Uninterruptible Power Supply (UPS) and two 225 KVA Power Distribution Units (PDUs) connected to remote power panels on the floor. The PDUs were originally installed for redundancy but have now exceeded their thresholds, meaning neither would be able to handle the load should the other fail.

Since the PDUs have exceeded their thresholds, there is no failover or redundancy if the PDUs fail. On October 31, 2014, OIT's Chief Operating Officer issued a moratorium on the installation of new equipment in the OARS data center. Exceptions for adding new equipment are granted if their power consumption can be offset by removing existing equipment from the data center.

Support for Mission Critical Applications

There are over 400 server applications labeled as mission-critical within the State of New Jersey's information technology infrastructure. Our surveys and interviews of 24 state agencies,

many of whom possess multiple mission-critical server applications, revealed only four are backed up and have redundancy at the OARS.

Recommendation

The deficiencies at the OARS noted above need to be corrected or compensated for in some manner. The OIT should also conduct a cost and feasibility study to determine if the OARS should be upgraded to properly accommodate disaster recovery efforts for all of New Jersey's truly mission-critical applications, or if outsourcing to vendors, or a combination of the two, would be more cost effective to accommodate New Jersey's disaster recovery needs.

Agencies' Contingency Plans

Many contingency and disaster recovery plans are not current and have not been tested.

Twenty-four agencies were reviewed to determine if their contingency plans are current and have been tested. From a survey and interviews with agency staff, it was determined that all 24 agencies do have contingency plans, but five agencies' contingency plans are not current. It was further noted that of the 24 agencies surveyed, eighteen have never tested their contingency plans.

The National Institute of Standards and Technology (NIST) Special Publication 800-34, Rev. 1, – *Contingency Planning Guide for Federal Information Systems* – 2.2.2 Continuity of Operations Plan, lists standard elements for a plan which include test, training, and exercise.

In addition, the OIT Policy 14-31 was issued in October 2014 and requires agencies to develop, maintain, and test a contingency plan for the critical systems identified in the Business Impact Analysis. The contingency plan is to describe the process for assuring the agency's ability to continue the critical business services and operations of each agency system, including systems used by branch or remote offices, and requires agencies to perform annual training and testing of the contingency plan to ensure all critical participants know their roles and responsibilities and to facilitate any needed corrections to the plan. Training and testing can be performed simultaneously.

The five agencies that have not updated their contingency plans risk having their plan fail and not being able to recover their mission-critical applications in a timely fashion. The 18 agencies who have never tested their contingency plans do not know if their recovery solutions will work during a real disruption. This could impact the recovery of their mission-critical applications and the public who may rely on these mission-critical applications.

Recommendation

The OIT is given responsibility for the information technology infrastructure of the executive branch by statute. Given their statutory responsibility for the provision and maintenance of the information technology infrastructure, the OIT should monitor, and assist where necessary, state agencies' efforts to update and test their contingency and recovery plans regularly.

State of New Jersey

CHRIS CHRISTIE
Governor

KIM GUADAGNO
Lt. Governor

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

DAVE WEINSTEIN
Chief Technology Officer

December 7, 2016

Mr. John J. Termyna
Assistant State Auditor
Office of Legislative Services
Office of the State Auditor
PO Box 067
Trenton, NJ 08625-0067

Re: Statewide Information Technology Contingency Planning Audit

Dear Mr. Termyna:

With regard to your audit report recommendations on the Statewide Information Technology Contingency Planning Audit at OIT, we would like to provide the following comments:

The Centralized Coordination of Contingency Planning recommendation specifically states:

> *"The OIT management should develop a methodology for monitoring and coordinating the contingency planning and recovery efforts of the executive branch. This should include regular input from all applicable agencies, and policies and procedures that will require the necessary follow-up, monitoring and support in testing the solutions."*

OIT's Contingency Planning process, also known as the Disaster Recovery Planning process, is currently being revamped to provide a more formalized methodology for implementing and exercising agency (including OIT) recovery plans. The new process is expected to more efficiently coordinate recovery efforts for systems hosted within OIT's infrastructure. Agencies are responsible for initiating the planning process with OIT. Agencies are also responsible for generating their own disaster recovery plan for systems not hosted within OIT's infrastructure.

The Agencies' Contingency Solutions Weaknesses recommendation specifically states:

> *"Agencies which lack proper fire suppression, water detectors, smoke detectors, UPS redundancy, or proper humidity or temperature controls should request funding for this equipment or work with the OIT to explore available options. Otherwise they risk total loss of production server room equipment. Agencies which lack computer room access logs or who do not change their server room access codes on a regular basis, need to promulgate policies instituting these controls to prevent unauthorized access."*

Prior to engaging in computer room expansion or retrofit projects, Agencies should consult with OIT to determine if the State's purpose built Enterprise Class Data Centers could provide the requisite data center service(s) at a reduced cost to the taxpayers.

The OIT Availability and Recovery Site (OARS) for its Operational Deficiencies recommendation specifically states:

> *"The deficiencies at the OARS noted above {1} need to be corrected or compensated for in some manner. The OIT should also conduct a cost and feasibility study to determine if the OARS should be upgraded to properly accommodate disaster recovery efforts for all of New Jersey's truly mission-critical applications, or if outsourcing to vendors, or a combination of the two, would be more cost effective to accommodate New Jersey's disaster recovery needs."*

{1} Private Ring Redundancy
There are several proposals under evaluation to address the single point of failure with the "private ring", which refers to the network between the Hub, River Road, and Hamilton Data Centers being at risk of a cable cut. The proposals OIT is evaluating to address the single point of failure include purchasing data communications services from a telecommunications carrier, purchasing dark fiber from the same, or constructing fiber that the State would own and maintain. OIT expects to be able to make a recommendation in Q4 of FY2017.

{1} Power Distribution Units
OIT is currently in the first phase of updating the OARS facility by adding redundancy to existing power. Project completion is anticipated in Q2 of FY2017. The second phase of this project will include adding redundancy to the existing UPS system for added protection. Project completion is anticipated in Q1 of FY2018.

In addition, OIT is currently researching various data center options to support Disaster Recovery for OIT and state agencies. This research includes:

- Financial and operational feasibility of upgrading the OARS facility by increasing power capacity or;
- Utilizing an existing state-owned data center facility as a tertiary site or;
- Leasing data center space from a vendor.

All options are currently under review. A final decision is expected in Q4 of FY2017.

{1} Support for Mission Critical Applications
The aforementioned projects and research effort for OARS will aid in addressing the "Support for Mission Critical Applications" for multiple state agencies.

The Agencies' Contingency Plans recommendation specifically states:

> *"The OIT is given the responsibility for the information technology infrastructure of the executive branch by statute. Given their statutory responsibility for the provision and maintenance of the information technology infrastructure, the OIT should monitor, and assist where necessary, state agencies' efforts to update and test their contingency and recovery plans regularly."*

OIT is currently vetting its inventory of more than 400 State systems to better refine the business criticality rating of each. Upon completion and, at the request of the using Agency, OIT will assist in building the recovery solution for any essential system hosted within OIT's infrastructure. This process is conveyed to all agencies during the System Architectural Review (SAR) meetings and is part of the SAR documentation.

OIT has increased its Disaster Recovery staff to better assist agencies with their Disaster Recovery planning and exercises.

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

Sincerely,

David J. Weinstein

Dave Weinstein
Chief Technology Officer

cc: S. Foundos
E. Rowe
H. Hottmann
O. Marcopolus