

**Mission:**

To protect, promote & improve the health of all people in Florida through integrated state, county & community efforts.



**Rick Scott**  
Governor

**John H. Armstrong, MD, FACS**  
State Surgeon General & Secretary

**Vision:** To be the Healthiest State in the Nation

## MEMORANDUM

Date: September 30, 2013

To: John H. Armstrong, MD, FACS, Surgeon General & Secretary

From: James D. Boyd, C.P.A., M.B.A., Inspector General 

Subject: R-1112DOH-010 - *Review of Information System Backups and Disaster Recovery Processes*

***All exempt and/or confidential information has been redacted from the public version of this report. Exempt information is only delivered to individuals appropriate to the activity that was reviewed. Requests to review or obtain the results of the exempt report content must submit a request to the Director of Auditing.***

### Executive Summary

The Department of Health (DOH), Office of Inspector General conducted a review of the processes for information system backups and disaster recovery efforts by the DOH Office of Information Technology (IT).

Based upon our review, we have made the following recommendations of IT management related to the scope and objectives of our project:

- Re-institute the receipt of the daily backup email reports in an automated process from the Southwood Shared Resource Center (SSRC) to ensure all unsuccessful backups are managed appropriately for data recovery and ensure compliance with agreed upon performance measures;
- (This issue has been redacted in accordance with Section 282.318(4)(f), Florida Statutes)
- Continue to revise and update the Continuity of Operations Plan for Information Technology (COOP-IT Plan) and reassess the criticality levels of all identified applications/systems, taking into account any changes to Mission Essential Functions identified by the Bureau of Preparedness and Response;
- Incorporate some Priority Level 3 applications/systems during disaster recovery exercises on an annual basis. This will provide better assurance that all applications/systems deemed critical and essential to DOH operations will be restored and functioning in a timely manner;
- Develop a written schedule that will include all planned tests for the next several years, ensuring that over a specific timeframe all critical and essential applications/systems (Priority Levels 1-3) will be tested to some degree. The plan should also include estimated funding and staff resources needed for each test and provide for at least some direct testing of application/system recovery during each fiscal year. This multi-year plan should be re-evaluated and updated at the start of each fiscal year;
- Ensure disaster recovery test exercises are recorded on the Testing and Lessons Learned Log, in accordance with the COOP-IT Plan; and
- Establish a timeframe in the COOP-IT Plan for the completion of all test results documentation following disaster recovery test exercises.

Details surrounding these recommendations can be found in the information provided below.

**September 30, 2013**

### **Scope and Objectives**

We reviewed the backup and disaster recovery processes utilized by DOH for information applications/systems managed by IT over the last three years. This review included those activities conducted by IT and the SSRC. We looked at the frequency of backups, the storage and security of the backup tapes and the frequency and type of disaster recovery exercises conducted.

DOH has undergone major reorganization over the last few years. As a result, efforts are currently underway by the Bureau of Preparedness and Response (BPR) to conduct a Department wide business impact analysis to help ensure the continuity of DOH's critical functions, including the identification of critical and essential applications/systems in the disaster recovery process. This will have an impact on IT's efforts to effectively restore essential information resources.

Thus, the following are examples of business processes that were excluded from this review:

- Business impact analysis - a study to prioritize the criticality of information resources for the enterprise based on costs (or consequences) of adverse events an impact analysis, threats to assets are identified and potential business losses determined for different time periods. This assessment is used to justify the extent of safeguards that are required and recovery time frames;
- COOP - plan used by an enterprise to respond to disruption of critical business processes; and
- Sufficiency of the disaster recovery testing efforts and results.

Furthermore, we did not examine or perform detailed testing of the following:

- System backups;
- SSRC security policies;
- COOP-IT test exercise plans;
- County Health Departments' COOP plans;
- Children's Medical Services Area Offices' COOP plans; or
- COOP plans for data systems not residing at the SSRC.

Once the business impact analysis is complete and changes resulting from the analysis are implemented, the Office of Inspector General reserves the right to conduct follow-up activities to conduct more in-depth reviews of the backup and disaster recovery processes.

### **Background**

Effective management of disaster recovery and data backups is more complex when the responsibilities over technology resources are split among multiple entities. Legislation mandates that the State of Florida consolidate agency data centers into concentrated quality facilities that provide the proper security, infrastructure, and staff resources to ensure the state's data is maintained reliably and safely, and is recoverable in the event of a disaster. As a result, IT has consolidated the majority of DOH headquarters data computing equipment and responsibility for data center operations to the SSRC.

As a part of the consolidation effort, DOH has entered into a Service Level Agreement (SLA) with the SSRC for backup services. According to the current SLA, backups are to be produced on a daily, weekly and monthly basis.

In July 2012, DOH implemented the Managed Services section of the SLA with the SSRC. Per Managed Services, the SSRC will also maintain DOH backup tapes for long-term storage. The long-term storage solution calls for backup tapes to be sent to a secure, offsite storage facility in Jacksonville for up to three years. Previous to this, DOH was responsible for all long-term storage of backup tapes.

**September 30, 2013**

Meanwhile, Information Technology Disaster Recovery Plans (ITDRPs) are information technology resources and procedures to ensure the availability of critical resources needed to support the agency mission in the event of a disaster and to return to normal operations within an accepted timeframe. The ITDRP takes into account availability requirements, recovery time frames, recovery procedures, back-up/mirroring details, systematic and regular testing and training.

Many people may be inclined to associate Disaster Recovery with a major type of event (i.e. hurricane, flood, fire, etc.). However, Disaster Recovery may also be needed in smaller events (i.e. server failure), since the term disaster more often refers to the potential results of a service disruption rather than the event causing the disruption. Thus, the purpose of a business continuity/disaster recovery is to enable a business entity to continue offering critical services in the event of a disruption and to survive a disastrous interruption to their critical and essential information applications/systems.

### **Findings and Recommendations**

During our review, we noted the following issues. For each noted issue, we have included a recommendation(s) for action to be taken by management. Management's response to each of our recommendations will be included in the final report.

#### ***Issue 1: Current backup notification processes do not provide assurance that backups are accurate and timely.***

---

Per the SLA, Attachment C, between IT and the SSRC, nightly (incremental) and weekly (full) backup of servers are to be performed by the SSRC. Attachment C of the SLA further defines the backup roles and the responsibilities of both the SSRC and IT. Two of the responsibilities of the provider (SSRC) are to 1) perform nightly backups and monthly archive backups and 2) ensure all backup processes are accurately and timely completed.

It was determined that prior to 2012, the SSRC provided a daily report via email to IT confirming successful and unsuccessful backups. The previous process included a review by IT to track successes and identify backup failures that required mitigation action. This provided a level of assurance that the backups were being performed as required by the SLA.

However, in December 2011, the IT staff member receiving these emails separated from IT and subsequently the position has not been filled. As a result, IT decided to suspend the receipt of the daily email. The justification for this decision was based upon the lack of staff resources to receive and review the report. IT made the decision for the SSRC to input any backup failures or other issues into the Numara Footprints system (a management database to track and compile project related service requests and complaints).

As a result of the absence of the daily email notification, IT is relying on SSRC staff to identify and report information system backup failures.

Per the SLA, Attachment C:

- The SSRC Service Responsibilities state it is the responsibility of the Provider (SSRC) to "Ensure all backup processes are accurately and timely completed" and "Inform Customers (DOH) of incidents or issues."

**September 30, 2013**

- The SSRC Performance Measures state, "The Backup Server will be available at least 99.5% of scheduled availability and provide 95.0% success rate on production data set backups."

Because IT is not receiving reports to identify whether issues are being logged into Numara Footprints, DOH is vulnerable to aborted back-ups being overlooked (intentionally or unintentionally) or dismissed. As a result of this, DOH risks the inability to restore all data in an emergency as well as monitor the performance of the SSRC's backup services to meet agreed upon measures. Discussions with the SSRC indicated that the email notification service could be re-instated and enhanced by way of an automated process.

***We recommend that DOH IT management re-institute the receipt of the daily backup email reports in an automated process from the SSRC to ensure all unsuccessful backups are managed appropriately for data recovery and ensure compliance with agreed upon performance measures.***

***Issue 2: THIS ISSUE AND THE ASSOCIATED RECOMMENDATIONS HAVE BEEN CLASSIFIED AS EXEMPT AND/OR CONFIDENTIAL IN ACCORDANCE WITH SECTION 282.318(4)(F), FLORIDA STATUTES AND THUS IS NOT AVAILABLE FOR PUBLIC DISTRIBUTION.***

---

Confidential material is only delivered to individuals appropriate to the activity reviewed.

All others who feel you have a justified purpose to view or obtain the results of this finding must submit a request to the Director of Auditing stating your name, business entity, current title, phone number, and the report number you are requesting. Please provide an explanation as to the reason for your request. Once approved, a time and date will be established for you to view the requested documentation under the supervision of the Internal Audit staff.

***Issue 3: The Continuity of Operations Plan for Information Technology (COOP-IT) Plan was last revised in 2010 and may not represent current applications/systems linked to mission essential DOH functions.***

---

*Information Technology Disaster Recovery Plan (ITDRP) Guidelines and Checklist*, published by the former Agency for Enterprise Information Technology, Office of Information Security in 2007, states, "The (disaster recovery) plan must be maintained and tested regularly."

Meanwhile, the COOP-IT Plan "establishes procedures to ensure availability of the technology required for mission essential Department of Health functions in the event of a disaster." Based upon the most recent plan provided by IT, this document was last updated June 30, 2010.

Furthermore, DOHP 50-10m-10 states, "The contingency planning process should identify critical functions; document practices for the backup, storage and retrieval of electronically stored information; and annually test the plans."

We recognize the current responsibility of DOH's overall COOP planning belongs to BPR. COOP efforts are based upon an identification and categorization of Mission Essential Functions (MEFs). Each MEF is to be categorized as to the criticality of the function and how quickly the function needs to be restored and operational in the event of a disaster or other large scale disruption to service. Tied to

**September 30, 2013**

this is the identification of critical applications/systems which support the each MEF. These applications/systems are separately evaluated as to their criticality (in conjunction with the criticality of the MEF) and are part of the COOP-IT Plan.

As a result of the recent DOH reorganization and efforts to update DOH's overall COOP plan by BPR, the COOP-IT Plan is currently outdated and does not provide confidence that critical and essential information applications/systems are properly identified and could be recovered timely.

Given the COOP-IT Plan was last revised in 2010, coinciding with the last time DOH updated their MEFs, the data is outdated. However, during our review, we discovered that BPR is currently conducting efforts to update the status of all current MEFs. IT staff is working closely with BPR staff to also update the COOP-IT Plan along with all associated applications/systems.

***We recommend that IT management continue to revise and update the COOP-IT Plan and reassess the criticality levels of all identified applications/systems, taking into account any changes to Mission Essential Functions identified by the Bureau of Preparedness and Response.***

***Issue 4: Testing of Disaster Recovery plans should involve a larger scope of applications/systems on a more frequent basis.***

---

The testing of applications and/or systems is an important element of disaster planning efforts. Rule 71A-1.012(5), F.A.C., states, "Information Technology Disaster Recovery Plans shall be tested at least annually; results of the annual exercise shall document those plan procedures that were successful and modifications required to correct the plan."

Meanwhile, DOHP 50-10m-10, VI., D., 1, states there is, "a requirement of state and federal law" for the agency to have a written COOP "that will provide the prompt and effective continuation of critical state functions in the event of a disaster, natural or manmade...Management must prepare, periodically update, and at a minimum, annual test a disaster recovery plan that will allow all critical information technology and communication systems to be available in the event of a major loss."

The COOP-IT Plan also mentions the requirement of at least annual testing of disaster recovery plans. However, this does not mean that only one test per year should be performed. In fact, IT staff recognizes that performing more than one test per year helps planning efforts since disaster recovery testing involves many different individuals, both from IT and the program unit owning the application/system. Additionally, multiple tests provide more focused testing on one (or a small group of) application(s)/system(s) as opposed to performing one large test per year that attempts to incorporate multiple applications/systems simultaneously.

As of August 5, 2013, IT reported 153 supported applications/systems. IT has assigned each application/system into one of five Priority Levels, based upon criticality and time needed for it to be placed back in operation in the event it needed to be recovered. Level 1 applications/systems are deemed to be the most critical while Level 4 are the least (Level 5 is typically assigned to new applications/systems that have not yet been evaluated).

In reviewing the way IT has defined the various criticality levels, Priority Levels 1 through 3 are applications/systems that have been determined to be critical or essential to operations of a business unit and thus are most important to the continuity of DOH operations.

The following table (Table 1) represents the breakdown of each of these categories and percentage of applications/systems from each which have been tested during the last three years:

**Table 1: Percentage of Applications/Systems Tested (by Priority level)**

Priority Level	Description	Total Applications/ Systems *	# of Applications/ Systems Tested **	% Tested
1	Mission Critical (one hour to one day recovery)	3	3	<b>100%</b>
2	Mission Essential (one day to one week recovery)	16	14	<b>88%</b>
3	Business Unit Essential (up to one month recovery)	42	0	<b>0%</b>
4	Important/Not Time Critical (recover as resources allow)	91	0	0%
5	New applications/systems not yet assigned (to be determined)	1	0	N/A
<b>Total</b>		<b>153</b>	<b>17</b>	

\* As of August 5, 2013

\*\* Tested during Disaster Recovery Exercises since August 2010

**Review of Information Technology's Data System Backup and Disaster Recovery Process**

Page 7 of 10

**September 30, 2013**

Details of each disaster recovery test performed during Fiscal Year 2010-11 through Fiscal Year 2012-13 can be found in Table 2 below.

**Table 2: Disaster Recovery Tests Performed by DOH-IT between FY 2010-11 and FY 2012-13**

<b>Date of Test</b>	<b>Level</b>	<b>Type of Test</b>	<b>What Was tested</b>	<b>Outcome</b>
<b>Priority 1 - Failover Test for Disease Control</b>				
August 23, 2010	1/2	Failover Test	Merlin, Single Sign-On, Business Objects, Integration Broker	Tests conducted, a write up (not a report) issued September 6, 2012
<b>Annual Disaster Recovery Exercise 2011</b>				
May 18-20, 2011	N/A	Full Recovery	IT Infrastructure (no applications/systems tested)	After Action Report issued September 23, 2011 , 7 findings
<b>IT Structured Tabletop Exercise</b>				
June 20, 2012	N/A	Tabletop Exercise	Update IT policy and procedures (no applications/systems tested)	After Action Report issued
<b>Failover Test</b>				
May 8, 2013	1	Failover Test	Merlin	After Action Report issued July 30, 2013, 2 issued identified and resolved
May 8, 2013	1/2	Failover Test	Cloverleaf/Integration Broker	After Action Report issued July 30, 2013, 2 issued identified and resolved
May 8, 2013	2	Failover Test	Single Sign-On	After Action Report issued July 30, 2013, 2 issued identified and resolved
May 8, 2013	2	Failover Test	Business Objects	After Action Report issued July 30, 2013, 2 issued identified and resolved
<b>Annual IT Disaster Recovery, Response &amp; Preparedness Exercise 2012-2013</b>				
May 14-16, 2013	2	Full Recovery	Absolute Forms Processor, Internet and Intranet websites, Serena Collage	Unknown
May 14-16, 2013	2	Full Recovery	CMS Child Assessment and Plan	Unknown
May 14-16, 2013	2	Full Recovery	Enterprise Geographic Information System	Unknown
May 14-16, 2013	2	Full Recovery	Food, Water & Vector-Borne Disease Surveillance System	Unknown
May 14-16, 2013	2	Full Recovery	Child Protection Team Information System	Unknown
May 14-16, 2013	2	Full Recovery	Exchange Mail System, Including Blackberry	Unknown
May 14-16, 2013	2	Full Recovery	Florida State Health Online Tracking System	Unknown
May 14-16, 2013	2	Full Recovery	Health Management System	Unknown
May 14-16, 2013	2	Full Recovery	Public Health Information Network Messaging System	Unknown
May 14-16, 2013	2	Full Recovery	Single-Sign-On	Unknown
May 14-16, 2013	2	Full Recovery	Business Objects	Unknown
May 14-16, 2013	2	Full Recovery	Integration Broker	Unknown
May 14-16, 2013	2	Full Recovery	Report Viewer	Unknown
<b>Failover Test</b>				
June 12, 2013	1	Failover Test	E-Vitals	After Action Report issued July 30, 2013

**September 30, 2013**

During the course of our review, we spoke with program staff involved in the Annual IT Disaster Recovery, Response & Preparedness Exercise 2012-2013 (May 14-16, 2013) who indicated they were unable to access the applications/systems and perform user testing as planned.

While 14 of 16 Priority Level 2 applications/systems have been included in disaster recovery testing during the last three years, two of DOH's largest and most critical systems, Health Management System (HMS) and COMPAS, have not been recently tested. Given the criticality and importance of these systems, IT should ensure that these systems be included in disaster recovery testing on a timely basis.

Furthermore, while IT management acknowledged Level 3 applications/systems were tested in the past, they have not been included in recent testing efforts. This came about as the result of a change several years ago in the timeframe established to recover Level 3 applications/systems being extended.

Certainly recovery time is an important factor in determining criticality of an application/system, but so too is the importance and dependence of an application/system to a given business unit. Since Level 3 applications/systems are labeled as "Business Unit Essential", they are deemed to be important to the operations of DOH and thus some level of testing and assurance should be provided for these applications/systems that they could be effectively recovered. Additionally, some IT staff who oversees disaster recovery testing also acknowledged that Level 3 applications/systems should be incorporated into disaster recovery testing efforts.

Meanwhile, it was noted during our review that some of the test exercises performed over the last three years (primarily in 2011 and 2012) were only a test of IT infrastructure and IT policy updates. Though structured walk-through tests are one of the primary industry-standard type of tests that can be performed, IT went two full years between tests that included actual recovery of DOH applications/systems. IT reorganization efforts, staff turnover, and funding issues during this time period played a part in the limited testing that was performed during these years.

Also, we were unable to ascertain whether IT management has a structured plan or schedule in place going forward to ensure that annual disaster recovery testing will include recovery of all critical and essential applications/systems.

Because recent disaster recovery testing exercises have omitted two critical Priority Level 2 applications/systems and all Priority Level 3 applications/systems, and for two consecutive years disaster recovery testing only involved tabletop exercises and updates to policy without actual system recovery, DOH remains vulnerable in the event these applications/systems were to suffer from an interruption of service.

***We recommend IT management incorporate some Priority Level 3 applications/systems during disaster recovery exercises on an annual basis. This will provide better assurance that all applications/systems deemed critical and essential to DOH operations will be restored and functioning in a timely manner.***

***Furthermore, we recommend IT management develop a written schedule that will include all planned tests for the next several years, ensuring that over a specific timeframe all critical and essential applications/systems (Priority Levels 1-3) will be tested to some degree. The plan should also include estimated funding and staff resources needed for each test and provide for at least some direct testing of application/system recovery during each fiscal year. This multi-year plan should be re-evaluated and updated at the start of each fiscal year.***

***Issue 5: IT does not consistently maintain documentation for all disaster recovery test exercises.***

---

During the review, we requested three fiscal years (FY 2010-2013) of IT's disaster recovery exercises required to be recorded on a log (Appendix 8 – Testing and Lessons Learned Log) per the COOP-IT Plan. Though IT was not able to produce the required log, they were able to provide a list of the exercises (See Table 2 above).

Additionally, we requested test results documentation that per the current COOP-IT Plan... "should be maintained about test exercises and any occurrences of disaster events (major to minor), including the date, type, and description of the event, as well as any lessons learned and corrective action. Corrective action should include a description of the action needed, the person responsible and the time frame for implementing the corrective action."

Test results documentation may take the form of a COOP-IT Test Results document or an After Action Report (for those tests that are part of the Homeland Security Exercise and Evaluation Program).

As of the end of fieldwork (June 27, 2013), IT was unable to provide to us five of the six test results documentation for disaster recovery tests conducted by IT during the Fiscal Years 2010-2013. It should be noted that on August 5, 2013, IT did provide test results documentation for four of the remaining five exercises performed during the last three fiscal years.

In reviewing the COOP-IT Plan, there was no specific mention of timeframes or deadlines as to how soon after a disaster recovery test should test results be documented. Because these documents were not available to us during our review fieldwork, it was difficult to understand the purpose of each test, the extent of testing performed, and the results of each test.

Test results documentation serve a valuable purpose. Primarily, they document the results of a given test exercise and should be used to document coordination of efforts to correct deficiencies noted during the exercise. This is vital to ensure the success of future test exercises and ultimately the recovery of critical and essential applications/systems.

***We recommend that IT management ensure disaster recovery test exercises are recorded on the Testing and Lessons Learned Log, in accordance with the COOP-IT Plan.***

***Furthermore, we recommend IT management establish a timeframe in the COOP-IT Plan for the completion of all test results documentation following disaster recovery test exercises.***

**Management's Response**

**Issue 1: Completed.** DOH IT has re-instituted the receipt of the daily backup email report from the SSRC. The report is being coordinated through our SLA Coordinator.

**Issue 2:**

Management's response has been classified as exempt and/or confidential in accordance with Section 282.318(4)(F), Florida Statutes and thus is not available for public distribution.

## **Review of Information Technology's Data System Backup and Disaster Recovery Process**

Page 10 of 10

**September 30, 2013**

**Issue 3:** We concur. **Anticipated Completion date:** March 31, 2014

DOH IT will revise the COOP-IT Plan to bring current standards identified by the Florida Division of Emergency Management. We will reassess the criticality levels of all DOH applications as they relate to the Mission Essential Functions identified by DOH divisions and program offices.

**Issue 4:** We concur. **Anticipated completion date:** March 31, 2014.

IT management will create a multi-year plan to test all priority Level 1-3 applications.

**Issue 5:** We concur. **Anticipated completion date:** March 31, 2014.

When revising the COOP-IT Plan, we will establish a timeframe for which all reports, documenting the disaster recovery exercises, must be completed. We will ensure that all disaster recovery exercises are documented appropriately and the *Testing and Lessons Learned Log* is maintained.

### **Closing Remarks**

This review was conducted by Office of Inspector General audit staff Kim I. Rolfe, Certified Government Auditing Professional, Management Review Specialist; and reviewed by Michael J. Bennett, Certified Internal Auditor, Director of Auditing.

We want to thank management and staff of Office of Information Technology and the Division Emergency Preparedness and Community Support, Bureau of Preparedness and Response for providing their cooperation and assistance to us during the course of this review.

Copies of final reports may be found on our website: [www.doh.state.fl.us/ig/Audit.htm](http://www.doh.state.fl.us/ig/Audit.htm)

Questions or comments related to the information provided in this report should be addressed to the Director of Auditing, Florida Department of Health by the following means:

Address: 4052 Bald Cypress Way, Bin A03  
Tallahassee, FL 32399

Email: [InspectorGeneral@doh.state.fl.us](mailto:InspectorGeneral@doh.state.fl.us)

Phone: (850) 245-4141

JDB/kir

cc: J. Martin Stubblefield, Deputy Secretary for Administration  
Bob Dillenschneider, Chief Information Officer