AUDIT OF THE INFORMATION SYSTEMS CONTINUITY PLAN

Report No. 10/11- 01

July 13, 2010

CONFIDENTIAL REPORT NOT FOR PUBLIC DISSEMINATION
PURSUANT TO SECTION 282.318(4)(f), F.S.

FIU FLORIDA INTERNATIONAL UNIVERSITY

OFFICE OF INTERNAL AUDIT

Date: July 13, 2010

To: Min Yao, CIO & Vice President of Information Technology

Dr. Kenneth Jessell, Chief Financial Officer/Senior Vice President of Finance and Administration

From: Allen Vann, Audit Director Allen Vann

Subject: **Audit of the Information Systems Continuity Plan**
Report No. 10/11-01

We have completed an audit of the Information Systems Continuity Plan. Our audit revealed that a comprehensive University-wide information systems continuity framework needs to be developed and implemented. Current disaster recovery plan, need to be tailored to address different threats and should be updated employing business impact analysis techniques to better understand the University's vulnerabilities. Finally, our review disclosed that there are infrastructure related issues effecting information systems continuity that need to be addressed. Management agreed to implement the ten resulting recommendations.

We wish to express our appreciation for the cooperation and courtesies extended to us by the Division of Information Technology and the Office of Emergency Management while conducting the audit.

C: Albert Maury, Chair, and Members of the Finance and Audit Committee
Mark Rosenberg, University President
Douglas Wartzok, Interim Provost & Executive Vice President
Javier I. Marques, Chief of Staff, Office of the President
Cheryl Granto, Information Technology Security Officer
Maria Rosa Drake, Director, Network Engineering & Telecommunications
Dorothy Miller, Assistant Director, Office of Emergency Management

BACKGROUND

The Division of Information Technology (IT) maintains an IT Disaster Recovery Plan (DRP). The DRP is a roadmap for staff to use to recover IT services in the event of a disruption. It includes relocating operations into a new location, and is intended to help minimize the impact of a major IT service interruption to key business functions and processes so that the University can continue to provide core services. To ensure continuous service and minimize impact of disasters, the University implemented an alternate backup facility located at the Northwest Regional Data Center (NWRDC) in Tallahassee, Florida. This offsite facility is used as a backup to the University's critical infrastructure and information and is sometimes used as an extension to the IT Division's primary physical facility. The University Division of IT reports to the Provost through the Chief Information Officer.

In addition, the Office of Emergency Management maintains an Emergency Management and Continuity of Operations Plan (EMCOP) and Policy that provides the roadmap for disaster prevention, response and recovery. Its purpose is to maintain the viability of mission critical operations during and after any emergency or other covered incidents. The Office of Emergency Management reports to the Office of Public Safety who in turn reports to the Provost through the Vice President for Student Affairs.

OBJECTIVES, SCOPE, AND METHODOLOGY

This audit was part of the approved work plan for the fiscal year 2009-2010. Our fieldwork was conducted from January 4th, 2010 through May 4th, 2010 and covered the University's Information System (IS) business continuity/disaster recovery plan as it existed on January 2010. The primary objectives of our audit were to ensure that in the event of a disruption, the University has adequate business continuity and disaster recovery processes for the resumption of IT services.

The University's IS Continuity Plan was evaluated to ensure that:

- Risks are appropriately identified and evaluated by focusing on impact on business processes for known and potential risks.

- There are adequate data backup and restore provisions.

- The disaster and recovery plan provides the basic framework for the recovery of IT processing capabilities in the event of a disaster.

- Manual interfaces to automated processes are identified, personnel are trained, and practice drills are conducted.

Our review covered IS continuity procedures in the following areas:

- Division of Information Technology (Division of IT)
- Graham Center
- University Health Services
- Engineering Information Center (EIC)
- The Wolfsonian
- College of Medicine
- College of Law
- and other departments.

This audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing and included tests of the records and such other auditing procedures as we considered necessary under the circumstances. The IS Continuity Plan was assessed using the Control Objectives for Information and Related Technology (CobiT), a set of best practices (framework) for IT management created by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI).

USE OF REPORT RESTRICTED

This report is intended solely for the internal use of Florida International University. This report contains the results of an internal audit of the information systems. Accordingly, per Florida Statutes section 282.318(4)(f), F.S. the results of this audit are confidential information and exempt from the provisions of section 119.07(1), which permits inspection of public records. This report may not be disclosed to a third party without the consent of the Office of Internal Audit.

FINDINGS AND RECOMMENDATIONS

1. IT Continuity Framework

A developed framework for IT Continuity supports business continuity management using a consistent process. The University developed the EMCOP as its framework. Florida Statute section 252 and the proposed State Board of Governor's (BOG) Campus Emergency Management Regulation 3.001 govern how the University develops its Emergency Management/Continuity of Operations Plan (COOP). The objective of such a framework is to assist in evaluating the required resilience of the University's infrastructure and to drive the development of disaster recovery and IT contingency plans throughout the University. The framework should address the organizational structure for continuity management, covering the roles, tasks and responsibilities of internal and external service providers, their management, and the planning processes that create the rules and structures to document, test and execute the disaster recovery and IT contingency plans of the University.

Emergency Management & Continuity of Operations Plan & Template are Ineffective for IT Continuity

In order to provide consistency and drive the development of disaster recovery and IT contingency plans across the University community the Office of Emergency Management (OEM) has developed a template to be completed by all campus units. The template, however, does not provide a sufficient structure for the creation of IT contingency plans for individual campus units as there are no instructions or requirements for campus units to create uniform DRP/IS Continuity plans that: 1) identify their critical IT resources; 2) monitor and report on the availability of critical resources; 3) consider alternative processing; and 4) consider backup and recovery.

Of the 7 campus units we examined, 6 did not complete and submit the template in 2009. The following were weaknesses found with the current framework based on units we examined along with their key databases/systems and potential effects:

- **Graham Center (GC):** According to their Computer Operations Manager, the Graham Center did not possess a disaster recovery plan that had been officially accepted by their senior management. He attributed this ostensibly to funding issues. On February 22, 2010, the Graham Center experienced a power outage due to a burnt electrical cable. The power outage brought down the Panther Card system affecting Panther Dining Services, Student Printing, access and tracking to FIU recreation areas, and other services throughout Modesto Maidique Campus (MMC) and Biscayne Bay Campus (BBC). Entry to the recreation centers had to be changed to a manual "visual match-up recognition" process.

The Panther Card system as well as phone services to GC were out for two days. The lack of a disaster recovery plan with specific procedures outlining the steps staff should take delayed the recovery. Since the GC did not have a detailed process in place for such an event, the decision to acquire a generator was not made until a day after the power outage occurred.

- **Engineering Information Center (EIC), College of Medicine, College of Law and College of Business:** None of the aforementioned campus units had a formal disaster recovery/IS continuity plan. These campus units all maintain at-risk data. For example:

    - College of Engineering and Engineering research
    - Applied Research Center's (ARC) research
    - Personal student information (testing, etc.)
    - Sensitive court case information.

    Though some procedures exist to prevent data loss, none of the campus units have documented procedures detailing how to recover their respective IS systems for different threat scenarios.

- **University Health Services (UHS):** UHS possessed a disaster recovery plan with procedures for their area of responsibility; however, the Coordinator of Computer Applications for their department acknowledged that the plan had not been updated since 2008. The plan does not provide for testing of backup tapes and systems.

Emergency Management and Continuity of Operations Plan Outdated and Incomplete

The Assistant Director of Emergency Management acknowledged that the plan was not up to date. The EMCOP plan was last updated December 1, 2008. The signature page in the EMCOP was outdated. It reflects an approval date of February 2004 by FIU's Executive Committee and the Executive Council. During our audit an updated Continuity of Operations Plan was submitted to the Florida Division of Emergency Management.

Systems and procedures listed within the plan such as the FIUnet modem no longer exist. The Emergency Management and Continuity of Operations Plan procedures, Section VI, Medical Emergencies, and Section VII, Hazardous Material Spills, Releases, or Emissions, are incomplete and contained blank pages with the words "No data available" printed on them. The plan was also missing procedures for disasters such as pandemics and cyber attacks, which are common in such plans. According to the Assistant Director of OEM, there was a pandemic plan that the "health services center was looking at," however, it is not incorporated into the University's Emergency Management and Continuity of Operations Plan.

Recommendations

The Office of Emergency Management should:

1.1 Consult with the Division of IT and develop a comprehensive, all-inclusive IT continuity framework.

1.2 Ensure that all campus units implement the IT continuity framework.

Management Response/Action Plan:

1.1 The Office of Emergency Management and the Division of IT will develop an IT Business Continuity framework. This framework will be incorporated into the COOP developed by the Office of Emergency Management.

Implementation Date: December 30, 2010

1.2 The Office of Emergency Management will engage the assistance of the CFO and the Provost to communicate and help ensure the various departments within FIU comply and implement the IT Business Continuity framework.

Implementation Date: January 30, 2011

2. IT Continuity Plans

Business Impact Analysis Needed

A critical first step in developing an Information Systems Continuity Plan is the performance of a Business Impact Analysis. During this analysis various events that could impact the continuity of operations and the various impacts to operations (financial, human, legal, reputational etc.) are identified. The analysis should identify the maximum tolerable outage for all critical systems and the objectives for when services should resume and from what point in time.

To its credit the Division of IT's Disaster Recovery Plan includes procedures for conducting a Business Impact Analysis at least twice a year. However, it is not evident that this analysis has been conducted. The Analysis should not be limited to the Division of IT but rather identify all critical areas of the University that would benefit from having information systems continuity procedures in place. For example, a Business Impact Analysis would have identified the vulnerability of the Panther Card system and established procedures to minimize down time to acceptable levels and rendered the system resilient to such an event.

Events, Recovery Strategies and Procedures Need Strengthening

Resumption procedures and strategies vary depending on the type of event/threat (e.g. hurricane, power failure, cyber attacks, pandemic, etc.). The Division of IT's DRP includes only one recovery strategy for all threats the University may face by employing an alternate site. The Division of IT did not have procedures for varied threats in the IS Continuity Plan. A good Information Systems Continuity Plan should include a set of different resumption procedures for events that may pose a threat on the critical systems of the University. These procedures are then tested for adequacy.

While the development of the alternate site at NWRDC is an appropriate strategy for many events, detailed backup procedures for different events would minimize delay and data loss for other types of threats such as sabotage caused by file alterations and cyber attacks.

The EMCOP and IT Disaster Recovery Plan do not include or reference the departmental EMCOPs or Information Systems Continuity Plans. The current IT Disaster Recovery Plan also does not include or reference the procedures for the individual teams involved in recovery activities, even though some of those procedures exist. A similar deficiency was noted in the State Auditor General's IT Audit conducted in 2007. The Auditor General noted that each "department had its own emergency response plan, but this information was not referenced from the disaster recovery plan."

Recommendations

The Division of IT should:

2.1 In consultation with the Office of Emergency Management routinely perform a Business Impact Analysis and update the Disaster Recovery Plan accordingly.

2.2 Identify all major events that could interrupt Information System service, tailor its emergency response procedures to each threat, and reference or include procedures for all of its critical recovery procedures in the DRP.

Management Response/Action Plan:

2.1 The Division of IT will develop a Business Impact Analysis that will be sent to all departments at FIU to assist in the identification of critical systems being managed by non-Division of IT departments and which are hosted outside the Division of IT's data center. The Division of IT will engage the assistance of the Provost and the CFO to communicate and help ensure that the various departments within FIU complete the Business Impact Analysis.

Implementation Date: December 30, 2010

2.2 The Division of IT will identify major disaster threats that could interrupt information system services. Some threats will require the same response and some will require unique response plans. Each plan will list which threats they cover.

Implementation Date: December 30, 2010

3. Critical IT Infrastructure and Backup Resource Issues

Our review disclosed that there are IS Continuity infrastructure related issues critical to building resilience in recovery situations.

Insufficient Infrastructure for Disaster Recovery Solutions

In March 2010, an Architect/Engineering firm, C3TS, engaged by Facilities Management to perform a data center study to assess the current "as-is" conditions of FIU data centers and server rooms reported that the University's infrastructure was wanting in the area of disaster recovery in the event of electrical outages and spikes. Facilities Management along with C3TS found that, "many systems lacked UPS battery backup, and led to many servers malfunctioning several times during power outages. These power fluctuations greatly reduced the life of several servers' hard drives that may store critical information." It was also noted in the Facilities Management's assessment that, "among the recurring deficiencies observed at most locations surveyed, was the lack of proper cooling systems and inadequate temperature/humidity control. Most of the buildings at the University were never designed to support server rooms." In addition, the report goes on to state, "some locations had surpassed the circuit breaker load capacity, and users resorted to running extension cords from multiple outlets in order to power all their equipment. As a result of these findings, many of the campus unit's efforts for disaster recovery are redundant and wasteful."

In addition, many of the campus units are not able to provide the proper environment to be able to have redundant power, e.g., areas that have generators in place are not able to use them as a solution to provide redundant power to their server rooms since they are only meant to provide power for emergency lighting, alarm systems, etc. and do not allow for enough energy to power the cooling systems needed for the server rooms and data centers to survive.

Outdated Backup Equipment

The following equipment present at NWRDC, according to acquisition dates and descriptions, given by their respective system administrators, are outdated, increasing the likelihood of backup system failures:

Server/ Component Name	Description	Acquisition Date
Solix2_DR	Hosts the University's UNIX web environment. Web sites like www.fiu.edu run on it.	07/25/2001

Server/ Component Name	Description	Acquisition Date
NFS_DR	UNIX version of network file shares (similar to shared drives); however it is shared to other servers only. It allows directories that contain web sites to be shared to multiple web servers, so that these systems can have a cluster of web servers running web sites.	04/04/2002
PSSCHED_DR	A PeopleSoft process scheduler, essential for PantherSoft.	06/28/2002
Brocade 1 & 2	Fiber Switches	09/17/2002
Brocade 3 & 4	Fiber Switches	10/22/2003
Regatta1	Runs PeopleSoft Application servers and a PeopleSoft DB server.	09/29/2002
PSFS_DR	PSFS_DR: The PeopleSoft File Server	01/07/2004

The Division of IT does not have a formal process to budget for and replace backup critical hardware used for disaster recovery. A log of backup hardware malfunctions and component replacements are not maintained by the Division of IT. Such logs could help identify hardware that need to be replaced to guarantee recovery efforts.

Recommendations

3.1 The Division of IT and Emergency Management should work with Facilities Management to assess the need for further investment in more resilient infrastructure, particularly power backup and cooling systems, at the University's decentralized data centers.

3.2 The Division of IT should develop as part of its disaster recovery efforts a routine for identifying and replacing outdated backup equipment.

Management Response/Action Plan:

3.1 Based on the results of the Business Impact Analysis, the Division of IT may recommend that critical systems be moved to the Data Center located in the PC building. The Division of IT recommends that instead of improving environmentals (power and cooling) at the large number of University decentralized data centers, a larger data center be built to support the current and future needs of the University. As shown by a study performed by an external consultant, FIU should start planning for a centralized University wide Data Center which would consolidate a lot of the equipment found throughout the University. In the long run, the investment in a centralized data will enhance the physical security of these systems.

Implementation Date: March 30, 2011

3.2 The Division of IT will develop refresh cycle which identifies equipment that needs to be replaced and when. Actual replacement of equipment will depend on available funding.

Implementation Date: December 30, 2010

4. Security of Disaster Recovery Data and Other Matters

Security of DR Data and Resources

The security of the systems at the NWRDC has not been assessed by the IT Security Office. Our vulnerability scans revealed that there were differences in the security policy for the local systems and the remote NWRDC site. The NWRDC Director stated that "FIU's equipment is not on the NWRDC network, but is on an extension of the FIU network managed by FIU staff. We provide space, physical security, and some remote hardware support." The Director indicated that it is up to FIU to ensure the security of the FIU systems at NWRDC.

The following vulnerabilities exist:

- The DR Center Firewall is not scanned on a regular basis. Security scans and penetration testing would mitigate potential risks to the data at NWRDC.

- The Disaster Recovery Plan does not include a security component. The IT Security Office or a third-party should assure and review significant changes to the Disaster Recovery Plan especially as it relates to the servers and data at NWRDC.

Background Checks not Performed on Key IT Staff

Many of the Division of IT's employees who have key roles in the disaster recovery process have not been subjected to background checks. The University does have a formal process of screening IT employees who have access to sensitive information upon being hired. However, many of the employees that work for the Division of IT who have a position of greater security, sensitivity or potential risk and are the gate-keepers of vast amounts of private and/or sensitive information, were found to not have been subjected to a background check. They include:

- Director of Network Engineering & Telecommunications
- Manager of Windows Systems Group for Enterprise Systems
- Assistant Director for UTS Operations & Enterprise Systems
- Coordinator for UTS Operations & Enterprise Systems
- Computer System Control Coordinator for Operations & Enterprise Systems
- OPS UTS employees who carry tape to and from tape library

Training

During our audit, we noted that the IT Security Officer does not emphasize IS Continuity and disaster recovery plans during the yearly IT security awareness training. In addition, the Assistant Director of the Office of Emergency Management stated that she as well as her staff were trained in emergency management but not specifically on business continuity. The University has in the past entrusted the Office of Emergency Management with business continuity in addition to emergency management. The Office of Emergency Management cannot effectively prepare the Continuity of Operations Plan because not all employees are trained or certified in business continuity.

Recommendations

The Division of IT should:

4.1 Include procedures for the IT Security Office or a third party to test the security and safety of disaster recovery resources and routinely scan the firewall and all disaster recovery servers located at NWRDC.

4.2 Request that Human Resources conduct background checks on IT employees who handle sensitive and/or personal information.

4.3 Include IT Continuity and Disaster Recovery Planning as part of the yearly IT Security awareness training.

The Office of Emergency Management should:

4.4 Train its staff on Business Continuity.

Management Response/Action Plan:

4.1 The ITSO has implemented regular scanning of the DR firewall. The DR environment will be included in our annual penetration testing. As far as the physical security and safety, this will be assessed on an annual basis as well.

Implementation Date: Immediately

4.2 The Division of IT will provide Human Resources with a list of all employees that handle sensitive and/or personal information so that a background check can be performed.

Implementation Date: August 30, 2010

4.3 The Division of IT will develop an IT Business Continuity and Disaster Recovery training that will be incorporated in the agendas for IT Security Awareness training (offered by the IT Security Office), Disaster Recovery training and Business Continuity training (offered by the Office of Emergency Management).

Implementation Date: December 30, 2010

4.4 An assessment of courses available will be completed through the Office of Emergency Management along with recommendations for courses to be taken by the emergency management group personnel. These will include courses offered online and in classroom settings.

Implementation Date: December 1, 2010