Internal Audit Department
Clerk of the Circuit Court • County Court • Board of County Commissioners
Post Office Box 7800, Tavares, FL 32778
Phone: (352) 253-1644 Fax: (352) 253-1645

June 22, 2011

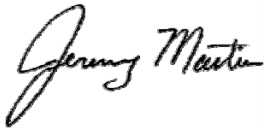
Steve Earls, Director
Lake County Board of County Commissioners, Information Technology
Post Office Box 7800
Tavares, FL 32778-7800

Mr. Earls:

As scheduled per the Clerk's Annual Internal Audit Plan, we have performed a follow up audit of BCC 2008-09 IT Business Continuity Plans dated June 19, 2008. Nineteen audit findings were contained in the original report and were reviewed in this audit.

We appreciate the cooperation and assistance provided by the BCC Information Technology department and other county entities contacted during the course of this internal audit.

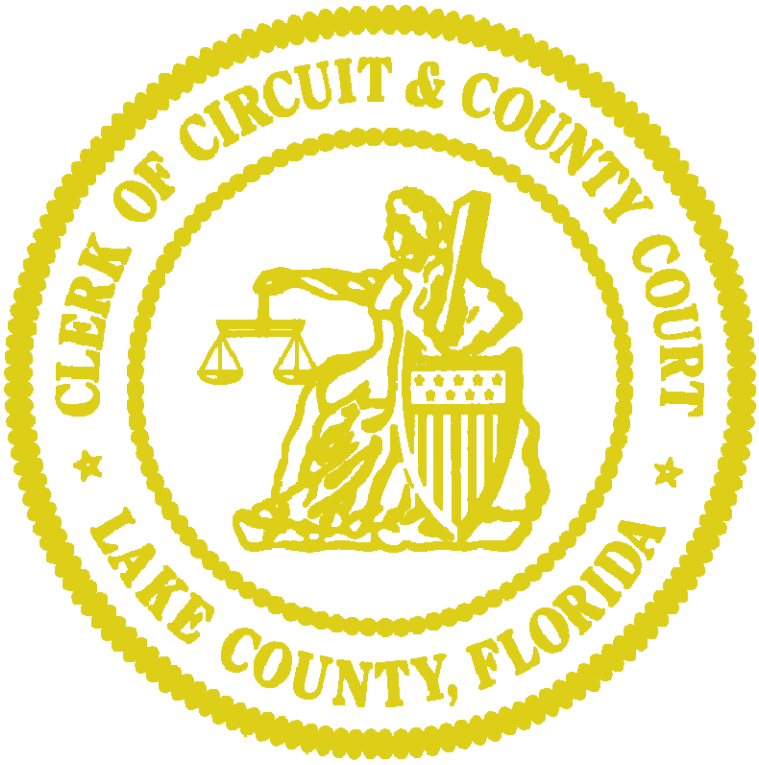
Sincerely,



Jeremy Martin, CPA
Internal Audit Director

JM/jh

cc: Honorable Neil Kelly, Clerk of Circuit & County Court
Board of County Commissioners
Darren Gray, County Manager



Internal Audit Department

BCC 2011-05
Follow Up to BCC 2008-09 IT Business Continuity Plans
Lake County Board of County Commissioners

June 22, 2011

Table of Contents

EXECUTIVE SUMMARY

OVERVIEW

The Lake County BCC Information Technology (IT) department is responsible for maintaining the County's computer systems and for backing up, storing and restoring data and the business to normal operations after a natural disaster or other interruption in business. Previously, the transportation and storage of data backup tapes was performed by Iron Mountain in Orlando, Florida. The County has cancelled the contract with Iron Mountain and now primarily stores the data backups on digital backup drives and for redundancy, uses backup tapes. Those backup tapes are transported by IT personnel and are stored in a vault at the Clerk's Public Records Center.

The Lake County Emergency Operations Center (EOC) is responsible for creating and disseminating emergency procedures to all areas of the BCC. Emergency supplies for safeguarding electronic equipment are stored in the IT department and are made available when the need arises.

SCOPE

Management desires to know if the management action plans agreed to in the original audit were implemented. The timeframe for this follow up audit was February – April, 2011.

OBJECTIVES

The objectives of this follow up audit were to:

1. Verify that the management action plans agreed to in the original audit were implemented effectively.
2. Determine if there have been any major changes to the process or organization since the audit and the effect of such changes.

OVERALL EVALUATION

During the course of the follow up audit IT personnel were cooperative and responsive to audit requests. We observed that IT personnel work well with one another, proactively seek ways to perform their duties more efficiently and take ownership of problems and progress towards problem resolutions. The IT department has made great strides in implementing new processes to take the place of those previously performed by Iron Mountain. They accomplished this by adopting a defined IT process framework for guiding them in establishing appropriate organizational bodies and structure and defining roles and responsibilities. They develop, maintain and train on IT contingency plans; and ensure data is backed up and restorations are tested. Potential threats and risks to the business are adequately identified and they are able to detect the circumstances under which the organization determines entering contingency status.

OPINION

Based on the results of our audit testing we are closing fourteen of the nineteen original audit findings, as they have been adequately addressed and corrective actions have been implemented. Five of the original findings remain open and should be addressed by County management as per the original audit recommendations. Additionally, we have opened two new findings with recommendations and have included them in the final report.

AUDIT BY:

Jeremy Martin, CPA, Internal Audit Director
Jacqueline Holder, CISA, CISM, Senior IT Auditor

SUMMARY OF ORIGNAL AUDIT FINDINGS

The following charts summarize the status of the original audit findings and the results as of the completion of the follow-up audit.

Open Findings - Control weaknesses that need additional corrective action.

Finding	Finding Description	Status	Comments
1	Procedures have not been established by County Management	Open	Due to changes in County management, little progress has been made in this area. The BCP function for County departments is the joint responsibility of the Emergency Operations Center Director and County IT. The preexisting IT COOP manual has been rewritten and is in the process of being edited for publication in the Summer of 2011.
2	No Alternate Site Agreements Established	Open	IT has been waiting to see what is going to happen with the new EOC. IT would like to be able to use a location within the new EOC as an alternate site. Plans are still in the works therefore no decision has been made.
3	Plan Testing (*is not being performed*)	Open	No full BCP tests, such as walk-throughs involving all key personnel, have been conducted. However, unplanned power outages and requests for data and database restores have given IT the opportunity to ensure their restore procedures are efficient and effective.
11	RPOs & RTOs Have not been Established	Open	Attempts were made to develop Recovery Point Objectives and Recovery Time Objectives however feedback from the individual departments was inconclusive. IT has asked for assistance in this area by means of an auditor assisted County Risk Assessment and/or Business Impact Analysis (BIA). Internal Audit has developed a Risk Assessment program that is currently being implemented.
12	Stored Media (*inventory is not accurate*)	Open	Tape inventory tracking still does not accurately reflect what is in storage.

Closed Findings - Control weaknesses for which corrective action has been completed to the auditor's satisfaction.

Finding	Finding Description	Status	Comments
4	Iron Mountain Security Cards (*are tampered with*)	Closed	The Iron Mountain storage facility is no longer being used therefore the original issue is closed. The new process of storing backup tapes does not involve the use of security cards.
5	Halon Fire Suppression System (*is overdue for inspection*)	Closed	The Iron Mountain storage facility is no longer being used therefore the original issue is closed. A new issue in this area was found with the new storage location. (See Findings and Recommendations Section of this report.)
6	Security and Confidentiality Requirements Not Specified	Closed	The Iron Mountain storage facility is no longer being used therefore the original issue is closed. A new issue in this area was found with the new storage location. (See Findings and Recommendations Section of this report.)
7	No call tree established	Closed	Call trees have been established for all areas of IT.
8	No Critical Systems Replacement Equipment & No Contract w/ Vendors	Closed	The most critical system within the County is the financial system, Munis. The Munis application and databases are maintained and backed up by the Clerk of Courts' Information Resources department. Policies and procedures for such are documented within the Clerk's Office. IT feels that the verbal agreements with vendors and availability of equipment with local retail vendors are sufficient for the needs of the County.
9	Employee training not documented	Closed	Training documentation is now being kept.
10	No right to audit clause (*in Iron Mountain contract*)	Closed	The Iron Mountain storage facility is no longer being used and there is no need for a contract as the Clerk of the Courts serves as the county auditor.
13	Truck Identification (*limits confidentiality*)	Closed	The Iron Mountain storage facility is no longer being used.
14	Emergency Disaster Preparedness Kits (*are not located within departments*)	Closed	Attempts have been made to assign this responsibility to the individual departments. However, the departments began using the supplies for everyday use (trash bags, batteries, etc.) IT has decided it would be best if they kept the supplies in a controlled area within the confines of the IT office.
15	Customer Authorization Form (*is not current*)	Closed	The Iron Mountain storage facility is no longer being used.
16	On-Line Customer Web Portal (*is not being used*)	Closed	The Iron Mountain storage facility is no longer being used.

Finding	Finding Description	Status	Comments
17	Lack of Underground Storage (*per contract with Iron Mountain*)	Closed	The Iron Mountain storage facility is no longer being used.
18	Different disaster scenarios (*were not covered by SOPs*)	Closed	This issue was closed during the original audit. Various SOPs were created.
19	Documentation of Test Results of Backup Databases (*was not being maintained*)	Closed	Database restore test results are being recorded in an Excel spreadsheet. There is room for improvement however, by additionally recording the actual results (pass/fail), any problems encountered and restore durations.

FINDINGS AND RECOMMENDATIONS

Backup tapes are not protected from water and/or fire damage.

Criteria: COBIT, a set of practices (framework) for information technology (IT) management, provides management and business process owners with an (IT) governance model that helps in delivering value from IT and understanding and managing the risks associated with IT. The COBIT control objective DS 4.9 (Delivery and Support) states that "...IT management should ensure that offsite arrangements are periodically assessed, at least annually, for content, environmental protection and security."

Condition: During the audit, we found that backup tapes are stored in a metal, filing-type, cabinet within a vault at the Public Records Center and all contents within the vault are protected from fire via overhead water sprinklers. This cabinet is not waterproof or fireproof.

Effect: Backups tapes have the potential of being destroyed by water or fire.

Recommendation: We recommend that the backup tapes be stored in a waterproof, fireproof container as water and fire can damage tape media.

Management Response: We concur. Current budgetary restraints prohibit us from receiving the funding to procure a waterproof/fireproof cabinet this budget year. We will make the purchase in FY12. The future plan is to place these tapes in the EOC once it is completed. Now that the BCC has approved the project, we expect to have a place in the EOC for redundant servers, data storage, and a waterproof/fireproof tape storage cabinet. This new building (EOC) will be a major part of the Business Continuity Plan.

Backup tape storage is not secure and confidential.

Criteria: COBIT, a set of practices (framework) for information technology (IT) management, provides management and business process owners with an (IT) governance model that helps in delivering value from IT and understanding and managing the risks associated with IT. The COBIT control objective DS 11.6 (Delivery and Support) states that IT management should "Define and implement policies and procedures to identify and apply security requirements applicable to the receipt, processing, storage and output of data to meet business objectives, the organisation's security policy and regulatory requirements."

Condition: During the audit, backup tapes were found to be in an unlocked storage cabinet within the vault at the Public Records Center. This vault is accessible by various employees of the Clerk of the Courts, therefore backup tape storage is not secure and confidential from unauthorized personnel.

Effect: Possible theft or destruction of tape backups.

Recommendation: We recommend that IT management ensure that the backup tape storage cabinet is kept locked at all times to prevent unauthorized access.

Management Response: We concur. We'll have the lock on the cabinet replaced or purchase a new locking cabinet.