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

November 15, 2011

Steve Earls, Director of Information Technology
Post Office Box 7800
Tavares, FL 32778-7800

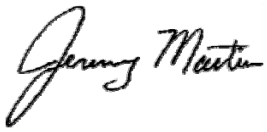
Mr. Earls:

As scheduled per the Clerk's Annual Internal Audit Plan, we have performed a follow up audit of BCC 2009-02 IT Active Directory dated April 9, 2009. Nineteen audit findings were contained in the original report.

Based on our follow up audit work and discussions with Leon Platt, Director, Information Systems, we are closing fifteen of the original audit findings. Our follow up audit indicated that these original findings have been addressed and adequate corrective changes have been implemented. The remaining four findings remain open and require additional corrective action.

We appreciate the cooperation and assistance provided by the Information Technology department during the course of this internal audit.

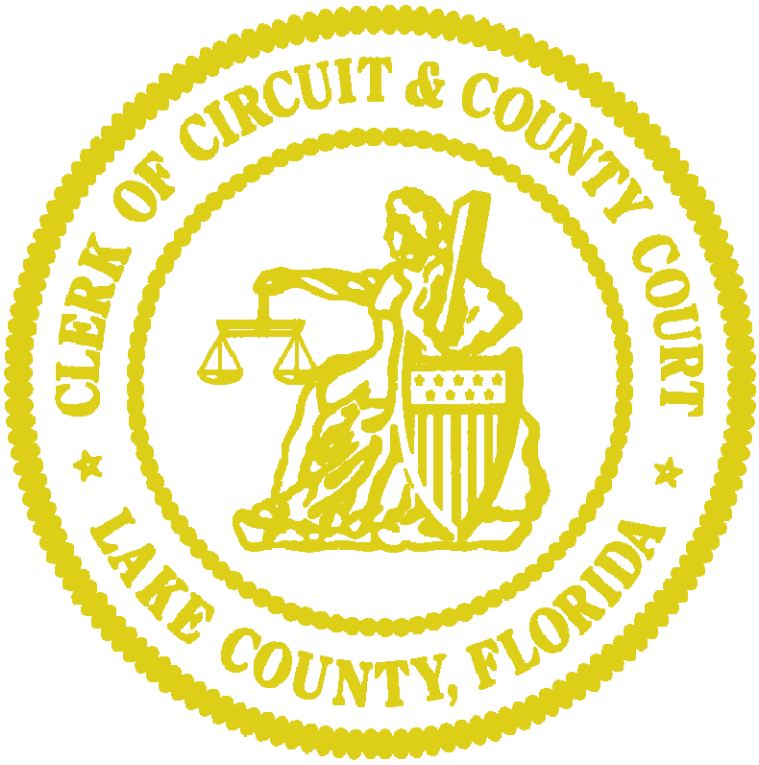
Sincerely,



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
Leon Platt, Director of Information Systems



Internal Audit Department

BCC 2011-04 Follow Up to BCC 2009-02 IT Active Directory
Lake County Board of County Commissioners
November 15, 2011

Table of Contents

EXECUTIVE SUMMARY

OVERVIEW

As requested by the County Manager and scheduled as part of the Annual Audit Plan, an internal audit was performed of the Active Directory Maintenance and Administration function of the Information Systems Division of the Information Technology Department. This was a follow-up audit to Audit Number BCC 2009-02, IT Active Directory.

Active Directory serves as a central location for network administration and security. It is responsible for authenticating and authorizing all users and computers within the County's network. It is additionally used for assigning and enforcing security policies, such as password requirements, for all users in the network and installing or updating software on network computers. For example, when a user logs into a computer, it is Active Directory that verifies his or her password and specifies whether he or she is a system administrator or normal user and what network resources he or she has access to, such as files, folders and applications.

SCOPE

County management desired to know if the management action plans agreed to in the original audit were implemented. The time frame of this audit was August 16, 2011 through September 27, 2011.

OBJECTIVES

1. To verify that the management action plans agreed to in the original audit were implemented effectively.
2. To 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 audit, we found the Division staff to work well together and to be focused on their duties. They strive to keep their goals in line with those of the County and their procedures are aligned with the best interest of the County in mind. Employees were very forthcoming with information and appeared to be eager to assist the auditors in any way. We were extended many opportunities to observe the staff during the normal course of their work. Management has addressed the majority of areas where improvements were recommended in the original audit and we commend them for doing so. The controls implemented are essential to improved accountability over the Division's operations.

OPINION

Based on the results of our audit testing, we have determined that the management of the Information Systems Division has effectively implemented plans supporting 15 of the 19 original

recommended changes. For those remaining issues, the auditee has stated that plans for remediation have been determined and will be implemented as soon as possible.

AUDIT BY:

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

SUMMARY OF ORIGINAL 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. Nothing came to the auditor's attention to warrant the creation of any new findings.

Open Findings - Control weaknesses that need additional corrective action.

Finding Number	Finding	Status	Comments
3	Domain controller is not patched against current vulnerabilities	Open	At the time of our initial audit testing, we found that one of the domain controllers was missing the latest updates. However, during the course of the audit, management installed the updates and implemented a plan to prevent this in the future. We believe their plan is adequate and we will follow up in 3-6 months to ensure it is functioning as designed.
11	Users exempt from changing their passwords on a regular basis	Open	During our audit testing, we found that several users were exempt from having to ever change their passwords. During the course of the audit, management addressed the problem accounts. We will follow up in 3-6 months to ensure the existing procedure is being followed.
12	Users/Accounts with old passwords	Open	During initial audit testing, we found that several accounts had old passwords. During the course of the audit, management addressed the problem accounts. We will follow up in 3-6 months to ensure the existing procedure is being followed.
13	Passwords cannot be changed for some user/accounts	Open	At the time of initial audit testing, we found that several accounts were not enabled to change their passwords. However, during the course of the audit, management addressed the problem accounts. We will follow up in 3-6 months to ensure the existing procedure is being followed.

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

Finding Number	Finding	Status	Comments
1	No Active Directory Policies and Procedures	Closed	Policy IS201 was created.
2	No established procedures for Domain Controller security updates	Closed	Policy IS202 was created.
4	Inadequate Account lockout policy	Closed	Account Lockout Policy is appropriate for the organization.
5	Inadequate Audit system events policy	Closed	Audit System Events policy has been corrected.
6	Inappropriate rights assignment to Authenticated Users group	Closed	Inappropriate rights assignment has been removed.
7	Domain Administrator & Administrators Groups	Closed	Inappropriate members have been removed from the group; membership is limited; recommended policy was created.
8	Inadequate Audit logon events policy	Closed	Audit Logon Events policy has been corrected.
9	Inadequate Audit Account logon events policy	Closed	Audit Account Logon Events policy has been corrected.
10	Inadequate Audit System events policy	Closed	Duplicate of Issue #5.
14	Passwords are not required for some users and accounts	Closed	Closed during the original audit.
15	Ineffective use of Group Policy for screen savers and/or passwords	Closed	Password protected screen savers have been enabled.
16	Lack of Policies and Procedures for GPOs	Closed	Policy IS101 was created.
17	Password change policy is inappropriate	Closed	Max and Min Password Ages have been rectified; recommended procedure was created.
18	Password quality is inadequate	Closed	Min Password Length and Password Complexity settings have been fixed; recommended procedure was created.
19	Logging on with Built-in domain Administrator accounts	Closed	Inappropriate members have been removed from the group; recommended policy was created.