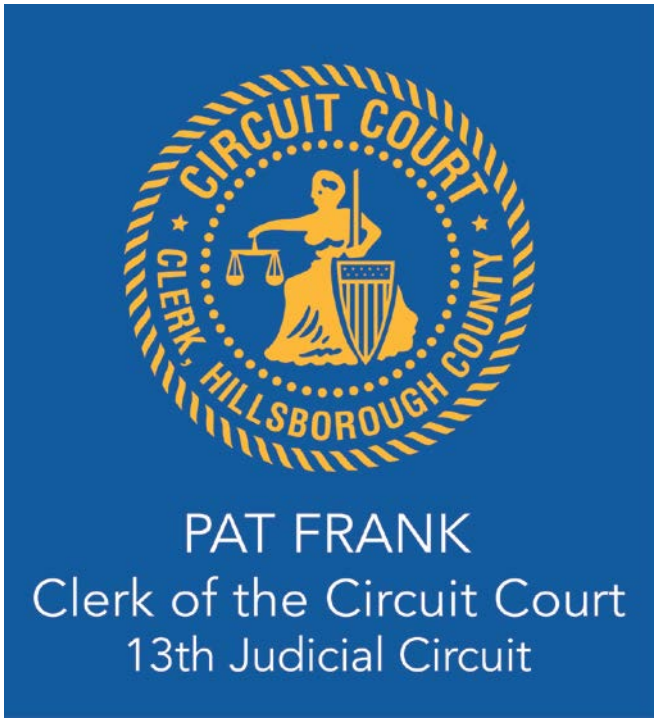


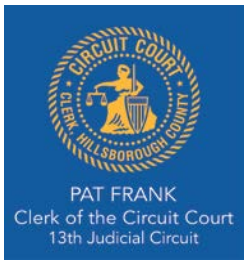
COUNTY AUDIT

HILLSBOROUGH COUNTY, FLORIDA

COMPREHENSIVE CASE INFORMATION SYSTEM (CCIS) ACCESS CONTROLS AUDIT

REPORT # 324

MARCH 17, 2017



March 17, 2017

Dear Pat Frank, Clerk of the Circuit Court and Comptroller:

The Audit Team performed an audit of the Comprehensive Case Information System (CCIS) Access Controls (Audit Report # 324, dated March 17, 2017). Responses to the Audit Team's recommendations were received from the Chief Deputy of Courts and the Senior Director of Court Systems Support and have been included in the Report after the audit comment and recommendations.

The purpose of this Report is to furnish management independent, objective analysis, recommendations, counsel, and information concerning the activities reviewed. It is not an appraisal or rating of management.

Although the Audit Team exercised due professional care in the performance of this audit, this should not be construed to mean that unreported noncompliance or irregularities do not exist. The deterrence of fraud and/or employee abuse is the responsibility of management. Audit procedures alone, even when carried out with professional care, do not guarantee that fraud or abuse will be detected.

The Audit Team appreciates the cooperation and professional courtesies extended to the auditors by the Chief Deputy of Courts and Senior Directors during this audit.

Sincerely,

Heidi Pinner, CIA, CISA, CRMA, CFE
Director of County Audit

CC: Doug Bakke, Chief Deputy, Courts
Kathleen Rocamora, Senior Director, Civil Courts
Brandi Williams, Senior Director, Criminal Courts
Idania Alfonso, Senior Director, Court Systems, Clerk's IT
Rick VanArsdall, Chief Deputy, Finance

TABLE OF CONTENTS

EXECUTIVE SUMMARY

BACKGROUND INFORMATION

The Florida Court Clerks and Comptrollers (FCCC) organization hosts an online database known as the Comprehensive Case Information System (CCIS) that is used to provide secure online access to court case data and driver and motor vehicle information. CCIS is a secured single point of search for state wide court case information, criminal history records, inmate data, and driver license information through links to the websites of the Florida Department of Law Enforcement (FDLE), the Department of Corrections (DOC), and the Department of Highway Safety and Motor Vehicles (DHSMV). The information that may be accessed through CCIS includes court case information, official records, and performance and accountability measures. Users of CCIS include the judicial community, state and local law enforcement, state agencies, Clerks of the Circuit Court and Comptrollers, and the Florida Legislature. The Hillsborough County Clerk of the Circuit Court and Comptroller (Clerk's Office) grants some of its employees access to CCIS with certain role permissions utilizing a username and password.

OBJECTIVE

The objective of the audit was to assess whether or not there are appropriate internal controls in place to ensure that the Clerk's Office use of the data maintained in CCIS is protected from unauthorized access, distribution, use, modification, or disclosure.

SCOPE

The audit was conducted in conformance with the *Generally Accepted Government Auditing Standards* and the *International Standards for the Professional Practice of Internal Auditing*. These Standards require that County Audit plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the audit comments and conclusions based on the audit objectives. County Audit believes that the evidence obtained provides this reasonable basis.

The audit scope included the controls in place for all CCIS users, both active and inactive, as-of November 4, 2016.

OVERALL EVALUATION

The management and employees of the Clerk's Office were responsive to the Audit Team's inquiries and provided the information requested in a timely and courteous manner. The Audit Team encountered knowledgeable and dedicated employees during the course of the audit.

AUDIT COMMENT	CONCLUSION OF OBJECTIVE	PAGE
1	There are opportunities to enhance CCIS access controls to reduce the risk of unauthorized access.	3

OPINION

The control environment relative to the user access controls over the CCIS system is at the repeatable maturity level. There is a need for increased controls to ensure active CCIS accounts exist for current employees who need the access. Formalized processes and procedures would be helpful to ensure user role permissions and overall CCIS usage is appropriate. In some cases, there is a need for the Clerk's Office to implement these controls for the first time. Addressing the improvement opportunities identified throughout this Report will enhance the overall control structure of CCIS user accounts through increased accountability, consistency, and sustainability.

The exit conference was held on March 3, 2017.

Other minor concerns not included in this Report were communicated to management and/or corrected during fieldwork.

AUDITED BY

Steve Hooper, CIA, CGAP, CCSA, CFE, Director of County Audit
Heidi Pinner, CIA, CFE, CISA, CRMA, General & IT Audit Manager
Ben Everett, CPA, CIA, CFE, Senior Internal Auditor

AUDIT COMMENT & RECOMMENDATIONS

AUDIT COMMENT

There are opportunities to enhance CCIS access controls to reduce the risk of unauthorized access.

Test Procedure

The Audit Team obtained a complete listing of the Clerk's Office CCIS user accounts. There were 168 accounts, including active and inactive users as of November 4, 2016. The Audit Team randomly selected 17 accounts (10%) from the list for a portion of the audit testing. Other audit tests were performed on the complete list of all users. The Audit Team conducted interviews and reviewed individual user activity logs to determine whether or not:

- Periodic user account reviews are performed by the Clerk's Office (complete list).
- User accounts were appropriately authorized (sample).
- User access role permissions are appropriate (sample).
- User access is terminated upon employee separation or re-assignment (complete list).
- User logins and inquiries appeared reasonably appropriate for business purposes (sample).
- User access inquiry dates and times were within normal Clerk business hours (sample).

Periodic User Account Reviews

An effective system access control is for administrators to periodically review the complete listing of user accounts to determine whether or not all active users still need access. The Audit Team obtained a listing which showed each user's last login date to identify accounts that have not been used within the last six months. Of the 168 users, there were 35 accounts whose last login date was six months old or longer, including 12 accounts that had no last login date recorded in the data. Twenty-five (25) of these 35 accounts were still active, while 10 had been deactivated. The FCCC has a CCIS Security Policy that requires CCIS accounts not accessed within a 30-day period to be deactivated. The Audit Team inquired with Clerk's Office staff and management and determined that periodic reviews of CCIS user accounts had not been performed.

Appropriate User Access Roles

Certain CCIS users have administrative rights to create, setup, and edit CCIS user accounts. The administrator grants access to some or all of the available role permissions by clicking checkboxes for each role in the administrator's setup screen. Prior to being setup with a CCIS account, new users must sign a CCIS User Security Agreement Form. The Audit Team reviewed the CCIS User Security Agreement Forms for the 17 accounts and found that all 17 users had properly completed and signed the form.

The Audit Team also reviewed the access setup screens for the 17 users in the audit sample for appropriateness. Fifteen (15) of the 17 users had been granted role permissions that were appropriate and consistent with other users in a similar job position. One user had access to several additional roles that management advised were not needed. Another user lacked access to a role that they did need. Each role permission has a short name label, but the meaning of the labels is not always clear. Based on interviews with Clerk's Office management, they are not clear on the exact meaning of each role name and what task it allows the user to perform. There is currently no formalized procedure to determine what roles a new CCIS user should be granted when their account is created.

Deactivating Access After Employee Separation or Re-Assignment

When an employee with an active CCIS account separates from the Clerk's Office, a help desk request is submitted to have the account deactivated by CCIS administrators. The Audit Team compared the list of 168 CCIS accounts to a complete list of all Clerk's Office employees to determine if any active accounts were for users who were no longer employed. Of the 168 CCIS accounts, 152 were active and 16 were inactive as of November 4, 2016. Of the 152 active accounts, 5 were former employees no longer employed by the Clerk's Office. No record of a request for deactivation could be found for those 5 employees.

The Audit Team compared the employee's termination dates to their last login dates in CCIS and found that no employees accessed CCIS after their last day of employment. The date when each inactive account was deactivated is not available in the CCIS system logs. Therefore, the Audit Team could not compare the timing of when CCIS accounts were deactivated to the last day of employment. There is currently no process in place to identify when an employee with CCIS access is re-assigned to a new job position and no longer needs the access.

Appropriateness of CCIS Use

The Audit Team reviewed activity log reports for each of the 17 users selected. These activity logs were for the 1-year period ending November 30, 2016. The logs consisted of only limited information including the date and time of access, internet protocol (IP) address, and which screen or module was accessed in CCIS. The logs do not show the case information, the name of the person queried, or what action was taken by the CCIS user. The FCCC was unable to provide the Audit Team with a more detailed log.

The Audit Team confirmed that all of the IP addresses in the usage logs for the sample were from the Clerk's Office network. The Audit Team also identified four instances where access times were on holidays, weekends, or outside of normal business hours. For those four instances, the Audit Team reviewed the employee's time card to determine the specific hours worked that day. All four instances were determined to have occurred at a time either before or after the employees' recorded hours. The limited amount of information in the access log made it unfeasible to determine the nature of this off-the-clock access. When interviewed by the Audit

Team, the employees indicated that they may have worked on job-related tasks before or after they clocked in for their assigned shift.

RECOMMENDATIONS

To enhance user access controls over the CCIS system, Clerk's Office management should consider implementing the following recommendations:

- Perform periodic reviews of user accounts and login dates to ensure active accounts are for current employees who need the access.
- Formalize a procedure to determine what role permissions should be granted to CCIS users.
- Implement a process to ensure separated or re-assigned employees have their CCIS access deactivated or updated, respectively.
- Perform periodic reviews of activity log samples to ensure that user access is appropriate.
- Reinforce to staff that work-related tasks should not be performed while employees are off the clock.

CLIENT RESPONSE: *Concur*

CORRECTIVE ACTION PLAN

- *User accounts will be reviewed and tracked on a monthly basis. Any account inactive in the last 30 days will be deactivated per the CCIS Security Policy.*
- *CCIS has changed their process from role based access to permissions based for a specific user. Going forward a procedure will be established whereby as an SM7 ticket is entered requesting CCIS access, the System Administrator, will send a CCIS security form to the Manager and/or Director to fill out with the permissions being requested for that employee.*
- *For current employees, the System Administrator will be meeting with the department Managers and Directors to review each employee's permissions and define the appropriate access needed. For staff that perform similar functions we will establish standard permissions for control and security purposes.*
- *Currently an SM7 ticket is provided from the department Directors for terminated employees. We will discuss putting a similar process in place for re-assigned employees. Once a month a report will be produced with a list of all active employees. This listing will be reviewed with the department Directors to catch any re-assigned employees or terminated employees that were missed.*
- *On a quarterly basis an activity log sample report will be requested of FCCC, this report will be used to compare an employees' activity vs permissions granted to ensure appropriate access.*
- *Staff will be notified that all work-related tasks should be performed while on the clock and in compliance with all existing policies and procedures.*

TARGET COMPLETION DATE: *07/01/2017*