COUNTY AUDIT DEPARTMENT

REPORT # 415

APRIL 6, 2023

An Audit of:

DATA WAREHOUSE

SYSTEM ACCESS CONTROLS

Cindy Stuart

CLERK OF COURT & COMPTROLLER
HILLSBOROUGH COUNTY

The Honorable Ken Hagan, Chair
The Honorable Donna Cameron Cepeda
The Honorable Harry Cohen
The Honorable Pat Kemp
The Honorable Gwen Myers
The Honorable Michael Owen
The Honorable Joshua Wostal

April 6, 2023

Dear Commissioners:

The Audit Team performed an audit of the Data Warehouse system access controls with the Health Care Services Department **(Audit Report #415, dated April 6, 2023**). Responses to the Audit Team's recommendations were received from Health Care Services. These management responses have been included in this Report.

The purpose of this Report is to furnish management with an independent, objective analysis, 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.

I appreciate this opportunity to be of service to the Board of County Commissioners. I am happy to address any questions that you may have or furnish additional information if desired.

Sincerely,

Heidi Pinner

Heidi Pinner, CIA CISA CFE CRMA
Chief Audit Executive, Clerk of Court & Comptroller

Equity. Transparency. Independence.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

BACKGROUND INFORMATION

As part of the annual audit plan, the County Audit Department performs periodic monitoring for user authentication and password access controls for the Board of County Commissioners and Clerk of Court & Comptroller information systems. As part of this ongoing assessment, the Data Warehouse system managed by the Hillsborough County Health Care Services Department was selected for review.

Data Warehouse is a comprehensive data management system used by the Health Care Services Department to gather large amounts of data, perform data analysis, and support business intelligence (BI) activities and reporting. Data Warehouse analytical capabilities allow Health Care Services to derive valuable business insights and improve the decision-making process.

OBJECTIVE

The objective of the audit was to determine whether or not general access controls are in place for the Data Warehouse system.

SCOPE

The audit was conducted in conformance with 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 scope of this review includes the logical access controls for the Data Warehouse system as of May 2022.

OVERALL CONCLUSION

The Health Care Services Department has ensured that most access security controls are in place for the Data Warehouse system. Two improvement opportunities were identified for user accounts and applicable access approval documentation.

PROCESS STRENGTHS AND SUCCESSES
- County system policies applicable to the Data Warehouse system are in place.
- Password configuration controls are properly established and working as intended.

RISKS AND OPPORTUNITIES
- User accounts may not be disabled in a timely manner.
- User access approvals have not been consistently documented.

Full testing results are included on page 4 of this Report.

The exit conference was held with County leadership on February 16, 2023.

OPINION

Control Maturity Levels

Informal | Repeatable | Formal | Managed | Best Practice

The overall control environment relative to Data Warehouse's access security controls is at a formal maturity level. This means that the controls are well defined, an overall control awareness exists, and procedures/processes with a formal structure are in place. Opportunities do exist to enhance this overall control structure by ensuring user account approvals are consistently documented and establishing a formal user access periodic review process.

AUDITED BY

Heidi Pinner, CIA, CISA, CFE, CRMA, Chief Audit Executive
Margaret Brown, CIA, Audit Manager
Raul Cardona, CIA, CISA, CSXA, Senior Internal Auditor

AUDIT COMMENT

DATA WAREHOUSE SYSTEM

MOST SYSTEM ACCESS CONTROLS ARE IN PLACE

Policies & Procedures Are Established

User Access is Reasonable Based on Title and Department

Password Security Controls Are in Place

Two opportunities for improvement were identified

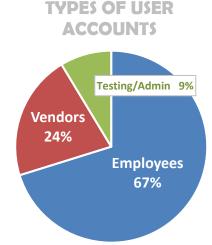To evaluate the system access controls in place for the Data Warehouse system, the Audit Team:

1. Performed interviews and inquiries with key process owners.

2. Reviewed policies and/or standard operating procedures for user provisioning and password security settings.

3. Reviewed Data Warehouse system password configurations to ensure that they comply with County Password Policy.

4. Evaluated the process in place to perform periodic reviews of user accounts.

5. Obtained the list of Data Warehouse user accounts on June 14, 2022 for testing:

   - Reviewed all user accounts to ensure user IDs were unique, in compliance with existing naming conventions and that account access was in alignment with job titles/duties.

   - Compared the user account list to the list of active employees to ensure that all employee user accounts belonged to active employees.

   - Selected a sample of 10 user accounts and requested documentation to verify user accounts were approved and the supporting documentation was properly maintained.

   - Followed up on identified generic, vendor and system admin accounts to ensure that they looked appropriate and are being used for their intended purpose.

TESTING RESULTS

The Audit Team obtained an understanding of Data Warehouse system access controls and how they are managed and supported by the Information and Innovation Office (IIO). County system IT policies applicable to the Data Warehouse user account provisioning, logging processes, and password security controls are in place.

The Audit Team identified 97 Data Warehouse user accounts:

- All user accounts (97) had a unique ID number.

- All employee user accounts (73) were based appropriately on the user's department and job title: Sixty-five (65) non-administrative users and eight (8) administrative users.

- One (1) of the 73 active user accounts belonged to a separated employee.

- Seven out of 10 (70%) user accounts in the sample did not have supporting documentation maintained for their access approval.

TYPES OF USER ACCOUNTS

Testing/Admin 9%

Vendors 24%

Employees 67%

- The system administration accounts and the one test account identified appeared appropriate and necessary.

- Currently, there is no periodic review of user's accounts access being performed at the network level.

RECOMMENDATION

HCS management should consider the following best practices to enhance the existing user access controls for the Data Warehouse system:

1. Ensure that any user account belonging to a separated employee or contractor is identified and disabled in a timely manner by the IT Department.

2. Ensure that user account approvals are consistently documented and supporting documentation is properly maintained.

CLIENT RESPONSE

1. Concur
2. Concur

CORRECTIVE ACTION PLAN

1. The Information Technology Department, in coordination with Health Care Services, is creating a management dashboard to enable Health Care Services managers and supervisors to review employee access to the Data Warehouse System and provide safeguards for timely deactivation. This process will also include a weekly email to managers with a list of Data Warehouse users for their review and action.

2. The Information Technology Department, in coordination with Health Care Services, created an electronic ticket system to ensure department management reviews employee access requests for the Data Warehouse System and establishes a formal approval process that documents the requestor, who the request is for, the level of access requested, and the date. The tickets will be created, approved, and reside in the Service Now module of the Technology Service Center.

TARGET COMPLETION DATE
*1. **04/28/2023***
*2. **Completed***

OTHER OBSERVATION

During the course of the audit, the Audit Team identified an area of improvement related to the periodic review of user access accounts in the Active Directory. Since this process is outside of the control of HCS and under the IIO's Information Technology Department, the following recommendation is being communicated to the Information Technology Department as an information security best practice for their consideration.

***Best Practice Consideration:** Implement a system tool to review Active Directory users' access and group memberships on a regular basis.*

There are system tools available such as *ManageEngine's ADManager Plus* that could be acquired in order to facilitate the periodic review of user access at the network level. In addition, *Microsoft Azure* offers an integrated feature (a Premium P2 license or Enterprise Mobility Security may be required) to set up recurring Active Directory user access reviews by roles, membership groups and/or applications.