



Cobb County...Expect the Best!

INTERNAL AUDIT DEPARTMENT

Report Number: 2022-01

***FINAL LETTER REPORT – Survey of Department
Application User Access Controls***

February 3, 2022

***Latona Thomas, CPA, CIA, Director
Erica Brooks Peters, CPA, Senior Internal Auditor
Tenaye Francois-Arneson, CIA, CFE, Senior Internal Auditor
Margarite Benevento, Senior Internal Auditor***

Table of Contents

Transmittal Memorandum	Page i
Background	Page 1
Assessment Results	Page 2
<i>Controls over User Access for Department Applications Need to be Strengthened</i>	Page 2
<u>The SharePoint Application List Needs to be Updated</u>	Page 2
<u>User Access Listings Need to Be Reviewed</u>	Page 3
<u>Recommendation 1:</u>	Page 3
Appendices	
Appendix I – Detailed Objectives, Scope, and Methodology	Page 5
Appendix II – Glossary	Page 6
Appendix III – Major Contributors to This Report	Page 7
Appendix IV – Final Report Distribution List	Page 8
Appendix V – Outcome Measures	Page 9
Appendix VI – Auditee’s Response	Page 10



COBB COUNTY INTERNAL AUDIT

Latona Thomas, CPA


100 Cherokee Street, Suite 250
Marietta, Georgia 30090
phone: (770) 528-2556
latona.thomas@cobbcounty.org

Director

February 3, 2022

MEMORANDUM

TO: Dr. Jackie McMorris, County Manager

FROM: Latona Thomas, CPA, CIA, Director 

SUBJECT: FINAL LETTER REPORT – Survey of Department Application User Access Controls

Attached for your review and comments is the subject final audit report. The overall objective of this review was to survey the system applications within Cobb County (the County) Agencies and Departments (Departments) to determine that user access is restricted to current employees, active contractors, or third-party vendors and to determine if the existing approach is adequate to prevent unauthorized access to County systems and data in a timely manner.

Impact on the Governance of Cobb County

The recommendation when implemented will strengthen the controls over Department application user access. While not included in the original objective, County leadership and citizens can be assured the County has a complete and accurate list of Department system applications and that access to those applications is limited to only current employees, contractors, or third-party vendors.

Executive Summary

We previously reviewed the controls over terminated employee user access and made recommendations¹ to strengthen the controls and disable access in a timely manner. As a result of the preliminary survey performed in that review, we determined to subsequently review user access for Department system applications with specific emphasis on those hosted offsite and are not behind the County's firewall. We started with a discovery sample of approximately 50% of the Department system applications selected to determine the accessibility of the reports, as well as the information that the reports would typically capture.

¹ Refer to Report #2021-004 'Review of Terminated Employees User Access Controls, issued August 26, 2021.

We also performed preliminary procedures on the discovery sampled system applications and identified some initial discrepancies between system application user listings and Human Resources (HR) list of current employees. Based on subsequent discussions and upon performing additional procedures, we determined that the County's list of Department system applications could not be relied upon for auditing purposes and needs to be reviewed and updated. Due to the data reliability issues identified, we concluded testing and did not perform the subsequent procedures to validate the list or review the Departments' processes.

Recommendations

We made one recommendation to strengthen the internal controls over Department system application user access and to validate the completeness and accuracy of the County's listing of Department system applications. For the specific recommendation, see the 'Assessment Results' section of this report beginning on Page 2.

Responding to This Report

The Chief Information Officer provided a response to our draft report and concurred with our recommendation. The complete responses to the draft report are included in Appendix VI with an expected completion date of August 2022. A copy of this report will be distributed as referenced in Appendix IV. We will perform a follow-up on the corrective actions one year from the date of this report. Please contact me at (770) 528-2559 if you have questions or Erica Brooks Peters, Auditor-In-Charge, at 770-528-2558.

Background

User access for County system applications may be granted to employees, contractors, and third-party vendors. Information Services (IS) is responsible for granting, disabling, or removing user access upon the User Department's request. The User Department is responsible for reviewing user access periodically to ensure that only current employees, contractors, and vendors have access to their applications and notifying IS of any required changes to access levels². In the 'Review of Terminated User Access Controls'¹ audit, we determined that user access to County applications that are hosted off-site are not behind the County's firewall which would prevent unauthorized access by former employees, contractors, and third-party vendors. Therefore, applications that are hosted outside of the County require that IS disable user access to these applications directly upon notification by County agencies, departments, or Elected Official offices. In addition, some hosted applications are set up with a Single Sign-On (SSO) feature which is tied to the County's Active Directory. In this case, when an employee, contractor, or vendor access is terminated in Active Directory, they are no longer able to access the application. For applications that are not set up with SSO, their access would remain active unless disabled separately by IS upon request by the User Department. In addition, contractors and third-party vendors would have to be disabled directly by IS upon request by the User Department as well.

Because this is a limited scoped project designed to identify and summarize processes within County Agencies/Departments, it is not designed to conclude on the completeness or accuracy of the list of system applications obtained. As such, any identified risks related to the completeness or accuracy of system applications will be discussed and analyzed as a potential audit lead.

The remaining of this page was left blank intentionally.

² Source: 'IS Technology User Account' and 'IS Technology Acceptable Use' Standards.

Assessment Results

Our objective of this review was to survey the system applications within County Agencies and Departments (Departments) to determine that user access is restricted to current employees, active contractors, or third-party vendors and to determine if the existing approach is adequate to prevent unauthorized access to County systems and data in a timely manner. Procedures involved included reviewing reports from Information Services (IS) and Human Resources (HR) Departments to identify the Department system applications and employees that use the selected applications. Using an initial discovery sample, we reviewed and compared the user access listings obtained from IS to the HR report of current employees. Additional planned procedures included: 1) Interviewing respective County departments to determine if the users not found on the HR list were current employees, contractors, or third-party vendors; 2) Requesting Departments to validate that their respective system application list from IS is complete and accurate; and 3) Evaluating the adequacy of Department processes around the review of user access for their applications and conclude on the results. However, while performing the initial testing procedures, we identified issues with data reliability and therefore, concluded fieldwork prior to performing these procedures. Based upon the information required to validate and update the application list, we determined that it would be more efficient if completed through the coordinated efforts of IS and the User Departments.

Controls over User Access for Department Applications Need to be Strengthened

The SharePoint Application List Needs to be Updated

The list of Department system applications has not been updated. Per initial discussions with IS, it is our understanding that the SharePoint list of department system applications had most recently been updated within the previous one to two years; however, further testing indicated only partial updates and not a comprehensive update as expected. Industry best practices indicate that the list of County applications should be reviewed and updated periodically, but at least annually. We determined that the list could not be relied upon for testing purposes and we are unable to conclude on the completeness and accuracy of the list of department system applications. Without an updated list of department applications that is reviewed and updated periodically with changes in personnel or based on changes in roles, responsibilities, functions, and business need, the following are increased risks:

- Unauthorized access to department applications and data could go undetected, resulting in improper changes or destruction of data, programs, or files.
- Employees or third-party vendors that no longer need access may gain access to department applications and data, resulting in improper changes or destruction of data, programs, or files.

User Access Listings Need to Be Reviewed

In our initial testing procedures, we observed that not all users on the select department application user listings were found on the HR list of current employees. The differences include employees from other County agencies, departments, or Elected Official offices; while others require additional procedures to substantiate. The IS Technology User Account Standards indicates that the Department Managers are responsible for requesting user rights for access to business applications and for identifying associated privileges. The IS Information Technology Policy and IS Technology Acceptable Use Standards indicates that Department management will determine and notify IS of required individual access levels. As stated previously, additional planned procedures were designed to determine whether or not the users not found on the HR report are active employees, contractors, or third-party vendors requiring access; and to evaluate their process of identifying, notifying, and subsequently validating the user access is appropriate. However, due to the data reliability issues indicated on the previous page, we judgmentally elected to discontinue testing prior to performing the additional procedures.

Effective monitoring controls over user access to system applications are essential to ensure that user access is terminated or modified as intended and in a consistent manner. Management reviews at the functional or activity level is a basic internal control activity which compares actual performance to planned or expected results. This activity must be ongoing to ensure expected management objectives and goals are met. These activities include approvals, authorizations, verifications, reconciliations, and the creation and maintenance of related records which provide evidence of execution of these activities as well as appropriate documentation.

Recommendation

The Chief Information Officer should:

Recommendation 1: Implement the following additional control mechanisms:

- Require Information Services Department Managers to coordinate with their respective assigned User Agencies, Departments, or Elected Official offices to update the SharePoint list of system applications. The list should be reviewed to ensure that all current applications are captured and that any applications that are no longer in use are removed or indicated as such.
- Require a periodic attestation from User Agencies, Departments, or Elected Official offices that the user access listings of their system applications have been reviewed and updated to ensure that only current employees, contractors, or third-party vendors have access to system applications. This attestation should be provided to Information Services at least annually and include a requirement that established processes be implemented within each User Agency, Department, or Elected Official office to notify IS of any needed changes to the access of their applications in a timely manner.

Auditee Response: Concur.

- Each Client Support Technology Services Manager will work with their assigned departments to update the county wide application list. All Technology Services Managers will review and update the IS specific applications. The initial update will be completed no later than April 1, 2022. An annual review will occur prior to April 1st of every year.

- Information Services will create an electronic sign off form for User Agencies, Departments, and Elected Official offices to attest their application user access list has been reviewed and updated. This form will be created no later than March 1, 2022. Information Services personnel will create application user lists and distribute to departments for review no later than June 1, 2022 and departmental review and sign off will be completed by August 1, 2022. This review will reoccur annually by August 1 of each year.

Detailed Objectives, Scope, and Methodology

We conducted this limited scope audit in accordance with The Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing. Our objective of this review was to survey the system applications within County Agencies and Departments to determine that user access is restricted to current employees, active contractors, or third-party vendors and to determine if the existing approach is adequate to prevent unauthorized access to County systems and data in a timely manner. Because this is a limited scoped project designed to identify and summarize processes within Agencies/Departments, it is not designed to conclude on the completeness or accuracy of the list of system applications obtained.

The work performed was limited to determining that user access is restricted to current employees, active contractors, or third-party vendors. This limited scope project covered certain applications on the SharePoint Application list.

Our limited assessment procedures included the following:

- I. Determining if user access is restricted to current employees and active contractors or third-party vendors:
 - A. Obtaining the list of County Applications from IS to determine the applications to select for review.
 - B. Obtaining the current employee listing from HR to compare to the user access listing for each application.
 - C. Inquiring of the Department/Agency leadership the applications used to validate the list from IS is complete and accurate.
- II. Determine if the existing approach is adequate to prevent unauthorized access to County systems and data in a timely manner:
 - A. Interviewing the Department/Agency leadership to gain an understanding of their process to review user access and determine if the existing approach is adequate to prevent unauthorized access to County systems and data in a timely manner.

Note: The final two testing procedures were not performed due to the data reliability issues identified in the previous testing procedures.

Glossary

User Departments	Refers to the County Departments that utilize applications managed by Information Services.
Single Sign On	Allows users to access multiple applications after entering their log in credentials once on a single page.
Active Directory	A database and set of services that connect users with network resources and enables administrators to manage user permissions and control access to network resources.
Microsoft SharePoint	A website used to securely store, organize, share and access information.

Major Contributors to This Report

Latona Thomas, CPA, CIA, Internal Audit Director
Erica Brooks Peters, CPA, Auditor-in-Charge

Final Report Distribution List

Kimberly Lemley, Chief Information Officer
Sharon Stanley, Support Services Agency Director
Jimmy Gisi, Deputy County Manager
Cobb County Audit Committee
Internal Audit Department File

Outcome Measures

This appendix presents detailed information on the measurable impact that our recommended corrective actions will have on County governance. This benefit will be incorporated into our annual report to the Board of Commissioners, Audit Committee, and County Manager.

Type and Value of Outcome Measure:

- Increased Safeguards over County Systems and Data – Actual; Recommendation, when implemented, will provide increased controls over County systems and data at the Department level (See Pages 2 - 4).
- Compliance with County Policy – Actual: Recommendation when implemented, will provide assurance that Departments review user access periodically (See Pages 2 - 4).
- Reliability of Information – Actual; Recommendation when implemented will provide assurance on the overall data reliability, as well as the completeness and accuracy of SharePoint Application List (See Pages 2 - 4).

Methodology Used to Measure the Reported Benefit:

This is based upon the known inherent risks related to user access and the benefits of strengthening the control environment around user access.

Auditee's Response



**COBB COUNTY
INFORMATION SERVICES DEPARTMENT**

100 Cherokee Street, Suite 520
Marietta, Georgia 30090-7000
770.528.8700 • fax: 770.528.8706
Kimberly.Lemley@cobbcounty.org

Kimberly B. Lemley
Chief Information Officer

DATE: January 21, 2022
TO: Latona Thomas, CPA, Director, Internal Audit
FROM: Kimberly B. Lemley, Chief Information Officer, Information Services
SUBJECT: Audit Response - Survey of Department Application User Access Controls

Several recommendations were made and our response to those recommendations are below.

Recommendation

The Chief Information Officer should:

Recommendation 1: Implement the following additional control mechanisms:

- Require Information Services Department Managers to coordinate with their respective assigned User Agencies, Departments, or Elected Official offices to update the SharePoint list of system applications. The list should be reviewed to ensure that all current applications are captured and that any applications that are no longer in use are removed or indicated as such.
- Require a periodic attestation from User Agencies, Departments, or Elected Official offices that the user access listings of their system applications have been reviewed and updated to ensure that only current employees, contractors, or third-party vendors have access to system applications. This attestation should be provided to Information Services at least annually and include a requirement that established processes be implemented within each User Agency, Department, or Elected Official office to notify IS of any needed changes to the access of their applications in a timely manner.

Response: [State: Concur, Disagree, or Concur with Alternate Solution]

Concur – Each Client Support Technology Services Manager will work with their assigned departments to update the county wide application list. All Technology Services Managers will review and update the IS specific applications. The initial update will be completed no later than April 1, 2022. An annual review will occur prior to April 1st of every year.

Concur – Information Services will create an electronic sign off form for User Agencies, Departments, and Elected Official offices to attest their application user access list has been reviewed and updated. This form will be created no later than March 1, 2022. Information Services personnel will create application user lists and distribute to departments for review no later than June 1, 2022 and departmental review and sign off will be completed by August 1, 2022. This review will reoccur annually by August 1 of each year.