RAUSCH
ADVISORY SERVICES

Infinite Campus Access Audit (FY19-11)

March 21, 2019

Ms. Connie Brown
Executive Director, Office of Internal Compliance
Atlanta Public Schools
130 Trinity Avenue, S.W.
Atlanta, GA 30303

Ms. Brown,

Rausch Advisory Services ("Rausch") is pleased to present the results of the Infinite Campus Access review (**FY19-11** Infinite Campus Access Controls).

The review was performed January 28, 2019 through March 1, 2019. The Executive Summary includes the scope, objectives, methodology, approach, and observations of the engagement as well as overall recommendations for Atlanta Public Schools ("APS").

Rausch appreciates the opportunity to have assisted in the review. If you have any questions or comments, please contact us at 404-775-1151.

Respectfully,

Pierre T Dait

Pierre T. Dait
Principal
Rausch Advisory Services, LLC.

Table of Contents

I. EXECUTIVE SUMMARY

We performed an audit of logical access to Infinite Campus (IC) which is Atlanta Public School's (APS) student information system. The purpose of the audit was to determine if the controls around IC access are sufficient to provide reasonable assurance that all users who are granted access to Infinite Campus have been properly authorized and appropriately role-restricted in their level of access. Our audit has allowed us to conclude with reasonable assurance that Infinite Campus access is well-controlled, but some improvements are needed.

The following issues requiring management corrective action were identified:

1. **536 Stale Accounts in Infinite Campus:** Out of the 6,932 employees and contractors with current access to Infinite Campus, there are 536 who have not accessed the application for a year or more. Of these, 146 no longer have Active Directory access to the network and thus have no access to Infinite Campus. The remainder remain actively employed at APS but appear to no longer have a need for IC access.
2. **The 2017 Infinite Campus SOC 2 Report Was Not Reviewed:** Although the Data and Information Group had reviewed Infinite Campus' previous SOC 2 reports, they had not reviewed IC's 2017 SOC 2 report, which was available in the first quarter of 2018. They have now requested, received, and reviewed the 2017 report and have requested the 2018 report as soon as it is available. Please note that there were no exceptions in that report and consequently APS had no exposure.

Management has agreed to all corrective actions recommended to address these improvement areas. Observations and related management action plans are described in greater detail in Section III of this report.

II. INTRODUCTION

Purpose

The purpose of the audit was to evaluate the adequacy of access controls for Infinite Campus which is Atlanta Public Schools' student information system.

Background

Logical security consists of software safeguards for an organization's systems, including user identification and password access, authentication, access rights and authority levels. These measures are to ensure that only authorized users are able to perform actions or securely access information in a network or a workstation. It is a subset of computer security.

At APS, the Data and Information Group (DIG), manages Infinite Campus including access and rights. An individual cannot be granted access to Infinite Campus unless he/she has active access to the APS network via Active Directory.

Lawson HR is the human resources information system used by APS. Data for all current district employees are maintained in Lawson HR.

The APS network is a Microsoft Windows network and utilizes Active Directory (AD) to restrict and control access. Active Directory is a directory service that Microsoft developed for the Windows domain networks. It authenticates and authorizes all users and computers in a Windows domain type network.

Please note that someone who is not activated within Active Directory cannot access Infinite Campus even if they have a live account in Infinite Campus. This provides an additional layer of control over access to the student information system.

Scope

Our scope was limited to controls over access to Infinite Campus at APS, covered the period from School Year 2015/16 through February, 2019. Excluded from our scope was student enrollment, a process through which access for IC is created for students and parents.

We reviewed vendor documentation, interviewed management, and performed tests with user data from three different applications: Infinite Campus, Active Directory, and Lawson HR. We executed our tests against data extracted from each of these three applications. We noted the following statistics as of February 25, 2019:

• Employees and contractors with network access through Active Directory	10,858
• Current district employees in Lawson HR	9,736
• Employees and contractors in Infinite Campus	6,932

Access to Infinite Campus

There are two interfaces available within Infinite Campus:

1. **Campus Application** – available to authorized school district employees and contractors
2. **Campus Portal** – for parents and students; there is no direct access to the application as the portal is separate from the campus application.

Infinite Campus users can be sorted into five general categories. The following section discusses each of these categories and describes how access is granted for each:

A. Students – Campus Portal

The Enrolling Adult completes and submits the New Student Enrollment Form. The enrollment form is reviewed, and the student's information is entered directly in Infinite Campus. Once entered, an IC account is established for the student. The system is programmed to grant students 'read only' access to specific fields in their own student record.

- If a student has more than 10 consecutive unexcused absences, DIG will contact the school to determine if the student should be withdrawn which will also terminate the student's access to IC.
- As part of their annual process, DIG will remove access to campus portal for all students after the end of the school year (all student data remains in the IC database) and reinstate the access to returning students at the beginning of the new school year.

B. Parents – Campus Portal

Parents are assigned a Parent Portal Activation Key that is unique to each of them and available upon request. Use of this key, will allow the parent/guardian to set up an account on the Web that will allow them indirect access to their student's records.

- Parents are granted 'read only' access to the student's academic record. However, they are allowed to initiate changes, subject to district approval, to certain fields such as demographic, health, and contact data fields.
- Parents/guardians need only sign-up for a campus portal account once and will have access to their student's records for the duration of the student's tenure at APS.

C. Staff – Campus Application

There are different tools available to users of Campus Application. Access to these tools is restricted by the groups, to which a user may be assigned. There are three types of groups:

1. Role-based groups – relate to job titles
2. Function-based groups – relate to Infinite Campus tools
3. Location-based groups – relate to the specific school

Each group will be granted access to a specific set of IC tools and, for each accessible tool, one or more of the four 'rights' available: Read, Write, Add, and Delete.

There are two ways to gain approval for staff access to IC:

1. Automatic approval: For new hires with job titles to which a predesignated IC role is assigned, a nightly computer job matches a comprehensive employee file from Human Resources to the access file in IC. This job will look for the following cases and make the appropriate changes to the IC access file:
   - Grants IC access to new employees with job titles which have a predesignated IC role.
   - Changes employee IC access for those employees transferring into a different job title which has a predesignated IC role.
   - Removes access for employees who have transferred into a job title for which IC access is unnecessary or who had their employment with APS terminated.

2. Managerial approval: When a principal or a central office manager determines that a subordinate needs IC access or access beyond that which they already have, he/she will sign a completed IC User Access form and submit it to the Data and Information Group for final approval.

D. Contractors – Campus Application

When an external contractor is engaged to perform a service, which requires access to IC, the contract owner must first approve the contractor's access to the network via Active Directory. Then the contract owner must sign a completed IC User Access Request form and submit it to the Data and Information Group. DIG will grant the contractor the appropriate level of access to IC. (There is further information regarding contractor access in the findings section below.)

E. Campus Administrators – Campus Application

The Campus Administrators are the Director and staff of the Data and Information Group. They are the only users who have full access to all of Infinite Campus. They are also the only users who have the ability to grant, modify, or remove access to Infinite Campus.

Note: The Data and Information Group will review the reasonability of any manual access request. They will also follow-up with questions as necessary. And, if approved, they will manually grant the access.

III. AUDIT METHODOLOGY

We followed standard internal audit methodology in performing the audit of logical access to Infinite Campus at Atlanta Public Schools. Through reviews of application documentation, interviews with key personnel, and observations we gained a good understanding of Infinite Campus and the processes in place to approve and grant logical access to the application. Through reviews of the processes used to grant access, we identified the manual controls in place to regulate logical access. We identified automated controls by careful review of application documentation. We designed and performed audit tests to determine if the controls are working.

Our testing included analysis of, and comparisons among, the data from three separate sources: Infinite Campus, Lawson HR, and Active Directory. We relied primarily on exception testing to identify any weaknesses within the IC control structure. (Exception testing is a procedure that is designed to identify cases where one or more controls may have failed.) The exceptions we found, along with our recommendations are detailed in the next section.

Please note that the exceptions we found are of low risk but nonetheless should be corrected by management to avoid a future problem that could arise.

IV. FINDINGS and RECOMMENDATIONS

1. There are 536 Stale Accounts Within Infinite Campus

Criteria: One of the basic principles of controlling logical access is to restrict access to the period of time during which the individual has a legitimate business reason for having that access.

Condition: There are 536 employees and contractors who have accounts in Infinite Campus but have not signed into the application during the past twelve months or longer. Of this number, 146 no longer have Active Directory access to the network and thus have no access to Infinite Campus. The remainder remain actively employed at APS but appear to no longer have a legitimate need for IC access.

Cause: There are multiple causes that may result in the access of employees and contractors not being terminated when their access is no longer needed.

A manager or principal may request access to Infinite Campus for a subordinate for whom there is a legitimate business reason for temporary access to Infinite Campus. (For example, when an employee is on sick leave it may be necessary to get access for a coworker to perform the sick employee’s duties within IC. But when that temporary reason ceases to exist (e.g., when a sick employee returns to work), the principal or Central Office manager may not inform the Data Information Group that the temporary access is no longer needed.

When a contractor is engaged and has a legitimate business reason for having access to IC, the manager to whom the contractor is reporting will submit a written request for that access. The SIS Access Request Form, however, does not require an End Date for the contractor's access. The Data Information Group has to rely on the APS manager to notify them when contractor access is no longer needed.

Effect: Failure to terminate access to Infinite Campus in a timely manner may potentially expose APS to violations of FERPA which could lead to reputational damage.

Recommendations:

1. Develop a policy that establishes the rules around the granting and removing of access to Infinite Campus for employees and contractors. Within that policy stipulate the number of lapsed days since last sign-on after which access will be removed. Distribute that policy to all principals and central office managers, who have subordinates with access to Infinite Campus.
2. Perform a periodic review of users' date of last access into Infinite Campus. Remove access for any users whose last sign-on exceeds the allowed number of lapsed days.
3. Add an 'End Date' field to the SIS Access Request Form and require it to be filled for all requests.

Management Corrective Action Plan:

By July 1, 2019 the following policies will be put into practice.

The Data + Information Group of Atlanta Public Schools (DIG) recognizes the importance of ensuring the safety of student data with the Student Information System (SIS). Consequently the following guidelines have been developed to ensure access to data with the SIS remains secure and appropriate, as well as, ensuring that the system itself is secure.

Internal Policy regarding access to the Student Information System

Guidelines for requesting access to the Student Information System

- Infinite Campus User Access Request Form is required for any staff requesting access to the SIS or requesting that their access be modified. As part of the approval process a supervisor is required to authorize the access request. The supervisor will also be required to indicate how long the staff member should have access by entering an end date on the form. If the user's access should remain for the entirety of the employee's tenure at that location/school, the supervisor will have option to indicate that access should persist.
- Prior to requesting access to the SIS, all users must have an Active Directory account, which will be used to provision access into the SIS. If the user is not an APS employee, the supervisor must follow the process to request an Active Directory account prior to submitting an Infinite Campus Access Request Form.

Guidelines for termination of access to the Student Information System

- All Infinite Campus staff and student accounts will be via the user's Active Directory credentials. This will ensure that as soon as a user is terminated or withdrawn the access will also be disabled.
- Any account not accessed within a 12 month period will be automatically deactivated. This will allow for users who only need to access the system annually (i.e. Summer School, summer registration, etc.) to retain access for those actions. After 9, 10 and 11 months of inactivity an email will be generated to users who are indicated as active employees by the HR system of record to the email address in the SIS notifying the user that per DIG policy, after 12 months of inactivity their user account will be disabled in the SIS.

2. The Infinite Campus SOC 2 Report Had Not Been Reviewed Every Year

Criteria: Vendors should be monitored and managed at a level commensurate with the risk they present to the organization. One of the important steps in monitoring and managing an IT vendor is to review the independent auditor's System and Organization Control Report (SOC 2). The SOC 2 report focuses on a business's non-financial reporting controls as they relate to security, availability, processing integrity, confidentiality, and privacy of a system, as opposed to a SOC 1 report which is focused on the financial reporting controls.

Condition: Although the Data and Information Group had reviewed previous SOC 2 reports, they had not reviewed Infinite Campus' SOC 2 report for 2017, which was available in the first quarter of 2018. They have now requested, received, and reviewed the 2017 report and have requested the 2018 report as soon as it is available.

Cause: Lack of a policy requirement that the Infinite Campus SOC 2 report be requested and reviewed every year when it becomes available during the first quarter.

Effect: There was no negative impact resulting from this oversight. However, with the almost constant change that is present among IT vendors there is always the risk of some loss of control at the vendor which may require APS to take some protective action.

Recommendation:

4. Develop a policy requiring that the Data Information Group obtain and review the SOC 2 report from Infinite Campus each year in February when the independent auditor issues it.

Management Corrective Action Plan:

Internal Policy regarding annually obtaining and reviewing the Infinite Campus SOC 2 report

Guidelines for requesting the annual Infinite Campus SOC 2 Report

- Data + Information Group (DIG) designated personnel will request the SOC 2 report, of the previous year, annually from the Student Information System vendor by the end of the first quarter of each year.
- Data + Information Group (DIG) designated personnel will review the Student Information System SOC 2 report annually within 30 days of the report being made available by the vendor.