



Internal Audit

Major IT Systems - PowerSchool Application Controls Audit

Major IT Systems - PowerSchool Application Controls Audit

Table of Contents

Executive Summary	3
Background	4
Scope	4
Objective	4
Methodology	4
Audit Observations and Recommendations	6
Observation 1: There is no documentation or monitoring of privileges and authorizations associated with user roles.	6
Observation 2: PowerSchool assigns present students the same value as students who have not had their attendance submitted.	7
Observation 3: Modification controls and edit checks are not implemented for grade calculations and assignments.	8
Observation 4: Passwords for substitute teachers do not adhere to District policy or best practices.....	9
Conclusion.....	11
Definition of Risk Level.....	12
Attachment 2.....	13
Management Response	13

Date: September 26, 2022

To: Board of Trustees
Stephanie S. Elizalde, Ed.D., Superintendent

From: Robert Rubel, MBA, CPA, CIA, CISA
Chief Internal Audit Officer

Subject: Major IT Systems – PowerSchool Application Controls Audit

Executive Summary

The Dallas Independent School District (District) Office of Internal Audit (OIA) has completed the Major IT Systems - PowerSchool Application Controls Audit.

The audit focused on the District's application controls for the PowerSchool Student Information System (SIS). The audit included reviewing application controls such as user access, passwords, and data modifications for PowerSchool SIS to determine if they are appropriate based on federal, state, and local policies, as well as industry best practices determined by the National Institute of Standards and Technology (NIST).

Overall, the Enterprise Applications group within the District's Information Technology department has implemented application controls for PowerSchool SIS. Opportunities for improvement were identified in the following areas:

1. There is no documentation or monitoring of privileges and authorizations associated with user roles.
2. PowerSchool assigns present students the same value¹ as students who have not had their attendance submitted.
3. Modification controls and edit checks are not implemented for grade calculations and assignments.
4. Passwords for substitute teachers do not adhere to District policy or best practices.

Implementation of the recommendations in this report could assist Enterprise Applications in strengthening PowerSchool SIS application controls.

¹ PowerSchool assigns certain values, or codes, for students as it relates to their presence or absence from a class period. While unexcused and excused absences have values, or codes, associated with the type of absence (i.e., U, E, etc.), PowerSchool does not have an assigned value, or code, for a student who is present or who has not had attendance submitted for them yet. Instead, attendance status for these students is represented by a null, or blank, value.

Background

The District implemented the PowerSchool Student Information System (SIS) during the 2018-2019 school year. Formerly, the District utilized Chancery Student Management System (SMS) to maintain student information. PowerSchool SIS is used to gather, validate, and report student information such as demographics, attendance, grades, etc. Certain student information within PowerSchool SIS is extracted and provided to the Texas Education Agency (TEA) for state reporting purposes. PowerSchool maintains data for approximately 145,000 students throughout 230 schools in the District. Enterprise Applications is responsible for maintaining the system and in conjunction with School Leadership determines processes for how PowerSchool SIS and PEIMS²-related activities operate at the district level.

PowerSchool is comprised of several different modules which are utilized for maintaining and tracking certain student information throughout the District. Auditors focused on modules pertaining to attendance and grading.

Scope

This audit focused on current operations and included activity from fiscal year 2021-2022; and certain other matters, procedures, and transactions outside that period were reviewed to understand and verify information during the audit period.

Objective

The objective of the Major IT Systems - PowerSchool Application Controls Audit was to review the district's application controls for PowerSchool SIS.

Methodology

OIA reviewed processes, controls, and supporting documents related to PowerSchool SIS. Auditors interviewed key personnel, conducted walkthroughs, and performed the following:

1. User Access - To determine whether access to student data within PowerSchool is appropriate auditors performed the following:
 - Auditors requested a listing of users with access to PowerSchool to compare to an active employee listing from HCM to verify that only current employees and substitutes have access to PowerSchool.
No recommendations were noted; however, the results were communicated to Enterprise Applications for further review.
 - Auditors requested a listing of PowerSchool user privileges and authorizations in order to compare to their job descriptions to determine if appropriate based on job responsibilities.
Recommendation 1 in this report was noted.

² Public Education Information Management System (PEIMS) encompasses all data requested and received by TEA about public education, including student demographic and academic performance, personnel, financial, and organizational information.

- Auditors reviewed PowerSchool configuration settings to determine if controls were implemented to prevent concurrent sessions and lock out users due to prolonged inactivity. No recommendations were noted; however, the results were communicated to Enterprise Applications for further review.
2. Password Controls - To determine if PowerSchool requires password protection and whether password requirements are adequate based on District policy or best practice standards, auditors reviewed password configurations in PowerSchool. Auditors focused on passwords for substitute teachers as District employees gain access to PowerSchool via Enterprise Active Directory (EAD). Recommendation 4 in this report was noted.
 3. Data Accuracy and Validity - To determine if controls are in place for verifying the accuracy and validity of data in PowerSchool auditors reviewed the following:
 - Auditors reviewed data outputs for grades and attendance. Recommendation 2 in this report was noted.
 - Auditors requested a listing of application edit checks (i.e., reasonableness and limit checks, sequence checks, built in cross-checks, automated validations, etc.) for PowerSchool data to determine if automated controls are in place for ensuring the accuracy of data. No exceptions were noted.
 - Auditors reviewed training materials for verifying accuracy of data and performed walkthroughs of processes at a selection of campuses. No exceptions were noted.
 4. Data Modifications - To determine whether modifications to attendance and grade data were appropriately performed and monitored by authorized staff, auditors reviewed configurations of gradebooks in PowerSchool along with processes for modifying attendance and grades. Recommendation 3 in this report was noted.
 5. Back Up and Recovery - To determine whether there are processes in place to effectively mitigate the potential for significant data loss within PowerSchool, auditors reviewed backup and recovery processes and requested a copy of the most recent backup. No exceptions were noted.
 6. Data History - To determine whether data is appropriately logged, and audit trails are established, auditors reviewed the audit log functions for grades and attendance data. No exceptions were noted; however, the results were communicated to Enterprise Applications for further review.

Primary criteria used for this audit were:

- 1) National Institute of Standards and Technology (NIST) Security and Privacy Controls for Information Systems and Organizations, September 2020
- 2) Federal Information System Controls Audit Manual (FISCAM), February 2009
- 3) 2021-2022 Student Data Services Operations Manual

Audit Observations and Recommendations

Observation 1: There is no documentation or monitoring of privileges and authorizations associated with user roles.

Condition

PowerSchool utilizes role-based access controls based on job function assigned via Oracle's automated processing information (API) function. OIA requested a copy of user roles for PowerSchool along with a listing of privileges and authorizations associated with each role in order to perform user access testing as part of the established audit program. Auditors noted that Enterprise Applications does maintain a listing of user roles; however, the listing does not define the privileges and authorizations associated with each role. Additionally, regular reviews of PowerSchool roles and associated authorizations and privileges are not performed to ensure appropriateness based on job responsibilities.

Criteria

CQ (REGULATION), Technology Resources, Issued September 1, 2020

Access to District technology resources will be managed as follows:

1. Every user must have a user profile that defines roles and access privileges.
2. The District will conduct reviews of standard users' access annually.
3. The District will conduct reviews of system administrator user accounts semi-annually.

National Institute of Standards and Technology – Security and Privacy Controls for Information Systems and Organizations, Section 3.1 – Access Control, AC-2 – Account Management

Define and document the types of accounts allowed and specifically prohibited for use within the system.

National Institute of Standards and Technology – Security and Privacy Controls for Information Systems and Organizations, Section 3.1 – Access Control, AC-3 – Access Enforcement

When users are assigned to specific roles, they inherit the authorizations or privileges defined for those roles.

National Institute of Standards and Technology – Security and Privacy Controls for Information Systems and Organizations, Section 3.5 – Configuration Management, CM-7 – Least Functionality

Organizations review functions, ports, protocols, and services provided by systems or system components to determine the functions and services that are candidates for elimination.

Cause

Enterprise Applications developed the most commonly used roles within PowerSchool during the implementation of the system in August 2018. During this implementation, each role began with view only permissions and was then granted certain privileges based on the job responsibilities of individuals

with those roles. However, as this assignment of authorizations and privileges was developed, Enterprise Applications did not fully document what authorizations and privileges were assigned to which roles. Internal audit obtained a spreadsheet from Enterprise Applications which appears to show an initial attempt at documenting these privileges, but it seems the effort was abandoned after a short time.

Effect

Lack of properly defined authorizations and privileges increases the risk of inappropriate access to PowerSchool and the data it holds. The absence of defined authorizations and privileges for roles makes it difficult to know exactly which roles are allowed to perform certain functions within PowerSchool. In addition, lack of documentation of these roles may cause an inability to monitor user authorizations and privileges and may result in users having certain authorizations and privileges based on outdated job responsibilities.

Recommendation 1

- Enterprise Applications should develop a listing of authorizations and privileges for each defined role within PowerSchool and ensure these are appropriate based on current job responsibilities.
- Enterprise Applications should implement processes for periodically reviewing roles within PowerSchool to ensure continued appropriateness based on job responsibilities. The review should include looking at any individual additional authorizations and privileges that have been granted outside the role-based access.

Risk Level: High³

Observation 2: PowerSchool assigns present students the same value as students who have not had their attendance submitted.

Condition

Auditors reviewed data outputs for grades and attendance. When reviewing attendance data in PowerSchool, auditors noted students who were recorded as present and students whose attendance had not been submitted were represented by the same value within PowerSchool. A null value is given for both scenarios within student files and for data reporting purposes.

PowerSchool is not able to show if attendance has been submitted for individual students; however, the system has the ability to identify when attendance has not been submitted via the Teacher Attendance Submission Status report. For unsubmitted attendance to be noticed, the report must be run for every campus on every day and then every teacher must be individually reviewed.

³ See Attachment 1 for Definition of Risk Level.

Criteria

National Institute of Standards and Technology – Security and Privacy Controls for Information Systems and Organizations, Section 3.19 – System and Information Integrity, SI-10 – Information Input Validation

Checking the valid syntax and semantics of systems inputs – including character set, length, numerical range, and acceptable values – verifies that inputs match specified definitions for format and content.

Cause

Per Enterprise Applications, PowerSchool does not allow for a separate value to be assigned for unsubmitted attendance. The system allows two options with regards to recording attendance: positive attendance or negative attendance. Positive attendance gives every student the value of present initially in each class, requiring the teacher to change the value if the student is absent. Negative attendance gives every student the value of absent initially in each class, requiring the teacher to change the value if the student is present.

Effect

Assigning a single value for two separate events prevents the data from distinguishing which event actually occurred. As it relates to attendance, the single value prevents the District's ability to efficiently determine which students were actually in attendance versus which have not had attendance taken.

Recommendation 2

- Enterprise Applications should explore options that will allow them to distinguish between unsubmitted attendance and students marked present.
- Enterprise Applications should consider the use of a data visualization software to aggregate unsubmitted attendance data from each campus to more effectively track the submission of attendance districtwide.

Risk Level: Medium⁴

Observation 3: Modification controls and edit checks are not implemented for grade calculations and assignments.

Condition

Auditors reviewed configurations of gradebooks in PowerSchool along with processes for modifying attendance and grades and noted that due to lack of application controls for modification of assignment categories, the potential for errors in grade calculations is increased. In addition, due to lack of system edit checks, there is no efficient way to identify if a calculation is incorrect.

Assignment categories are the types of assignments (i.e., homework, classwork, tests, etc.) that students are given to perform and subsequently graded on. Assignment categories are created at the

⁴ See Attachment 1 for Definition of Risk Level.

District level in an attempt to standardize the format for assignments and grading calculations. Each established assignment category is also given a correlating weight pre-determined by the District. The established weight for each assigned category is then pre-configured into the gradebook. When a teacher selects a pre-determined assignment category and inputs a grade, the gradebook automatically calculates the student's overall grade. Auditors noted that PowerSchool allows teachers to create their own assignment categories. When this occurs the pre-determined formula for calculating the student's average will not consider the teacher created assignments and correlating grades, therefore causing an inaccurate overall grade.

Criteria

National Institute of Standards and Technology – Security and Privacy Controls for Information Systems and Organizations, Section 3.19 – System and Information Integrity, SI-10 – Information Input Validation

Restricting the use of inputs to trusted sources and in trusted formats applies the concept of authorized or permitted software to information inputs. Specifying known trusted sources for information inputs and acceptable formats for such inputs can reduce the probability of malicious activity. The information inputs are those defined by the organization in the base control.

Cause

PowerSchool is configured to allow teachers to create their own assignment categories, rather than restricting them to ones pre-determined by the District.

Effect

When pre-configured assignment categories are not utilized, it results in the gradebook not calculating properly. This could result in a student's grade being incorrect.

Recommendation 3

- Enterprise Applications should consider implementing system controls within PowerSchool to restrict the ability for teachers to create their own assignment categories without prior approval.
- Enterprise Applications should consider adding system edit checks to identify errors in grading calculations.

Risk Level: Medium⁵

Observation 4: Passwords for substitute teachers do not adhere to District policy or best practices.

Condition

Auditors reviewed password configurations in PowerSchool noting that for District employees, access to PowerSchool is gained through the Enterprise Active Directory (EAD). There are processes in place to automatically update EAD access when employees are hired, separated, or other status changes occur.

⁵ See Attachment 1 for Definition of Risk Level.

Substitute teachers or other temporary employees are not given EAD access. As a result, Enterprise Applications has set up a separate access portal to PowerSchool for substitute teachers. This portal only allows the substitutes to view student names for the courses they are substituting for and permits them to record attendance for those students. Access to the portal is gained via a temporary password given by the campus. The temporary passwords are generated separately by each campus and should be reset each day. Auditors noted these temporary passwords are not unique to individuals and do not meet District policy or best practice standards for password security. In addition, auditors noted there are currently no monitoring processes in place to ensure these temporary passwords are reset daily.

Criteria

CQ (REGULATION), Technology Resources, Issued September 1, 2020

Passwords for District technology resources will be managed as follows:

- The District promotes the use of strong passwords, as defined by National Institute of Standards and Technology (NIST) Document SP 800-63-3.
- All District passwords must remain confidential and will not be shared.
- Passwords must have a minimum of 8 characters.
- Passwords must be stored and transmitted in an encrypted manner.
- District-owned mobile devices and Employee-owned mobile devices that allow access to District e-mail or any Confidential or Regulated data must be password protected in accordance with District standards.

National Institute of Standards and Technology – Security and Privacy Controls for Information Systems and Organizations, Section 3.7 – Identification and Authentication, IA-5 – Authenticator Management

Password-based authentication applies to passwords regardless of whether they are used in single-factor or multi-factor authentication. Long passwords or passphrases are preferable over shorter passwords. Enforced composition rules provide marginal security benefits while decreasing usability. However, organizations may choose to establish certain rules for password generation (e.g., minimum character length for long passwords) under certain circumstances and can enforce this requirement in IA-5(1)(h).

Cause

Due to the low-risk data and privileges associated with the substitute portal, Enterprise Applications has not required or enforced password controls for the PowerSchool substitute portal.

Effect

Inadequate password controls can leave a system vulnerable to unauthorized access. As a result, certain data could become compromised due to unauthorized modification or misuse. Auditors note that while the current data and privileges within the substitute portal are limited, if the portal was provided additional data and/or privileges the need for stronger password controls would be increased.

Recommendation 4

- Enterprise Applications should implement password controls for the PowerSchool substitute portal that adhere to District policy and best practices.

Risk Level: Low⁶

Conclusion

The District relies heavily on accurate grading and attendance data within the student information system; and, as such, it is crucial that application controls are implemented within PowerSchool SIS to effectively track, monitor, and safeguard student data.

Overall, PowerSchool SIS has some application controls surrounding student attendance and grades; however, implementation of the recommendations in this report could improve the security, accuracy, and validity of data within PowerSchool SIS.

We would like to thank Enterprise Applications and Student Data Services for their cooperation and assistance with this audit.

The audit was conducted in accordance with the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*. Those standards require OIA to plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our observations and conclusions based on our audit objectives. OIA believes the evidence obtained provides a reasonable basis for our observations and conclusions based on our audit objectives.

Respectfully submitted,

Robert Rubel

Robert Rubel, MBA, CPA, CIA, CISA
Chief Internal Audit Officer

Cc: Pamela Lear, Ed.D., Chief of Staff and Racial Equity
Dwayne Thompson, Deputy Superintendent, Business Services, Financial Services
Tiffany Huitt, Chief Schools Officer, School Leadership
Sean Brinkman, Chief Technology Officer
Marlon Harrison, Assistant Superintendent of Technology, Enterprise Applications
Michelle Thompson, Director I, Enterprise Applications, Technology
Carolyn Moreno, Manager Data Analysis, Enterprise Applications, Technology
Debra Hill, Director II, Student Data Services, Enterprise Applications, Technology

Acknowledgments:

Eva Narten, CPA, CIA, CISA, Deputy Chief, Internal Audit
Shelly Kelley, CPA, Audit Manager
Sam Willson, CFE, Auditor II
Rosa Lopez, CFE, Auditor I

⁶ See Attachment 1 for Definition of Risk Level

Definition of Risk Level

Risk Level	Definition
High	<p>High probability of occurrence that would significantly impact District operations and have a significant financial or compliance risk.</p> <p>These observations are defined as an issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of the District.</p>
Medium	<p>Risks are considered to be substantially undesirable and pose a moderate level of risk exposure to District operations. Without appropriate controls, the risk will happen on a consistent basis.</p>
Low	<p>The risks are considered to be undesirable and could moderately expose the District. Without appropriate controls, the risk will occur some of the time.</p>

Management Response

Observation 1 - There is no documentation or monitoring of privileges and authorizations associated with user roles.

Acknowledgement of observation:

- ☒ Agree
☐ Disagree

Management's Response:

While initial creation of page permissions is documented and processes are in place for PowerSchool end users to request additional access, as needed for the specific job responsibilities, there is not currently a single process or system that identifies the scope of page permissions.

To address this Observation, a PowerSchool district-level report will be developed by Dallas ISD Information Technology that identifies the page access for each Group/Role. An annual review of page access for each Group/Role and users assigned to that Group/Role will be conducted prior to July 1 each year. Based on annual review, appropriate page permissions will be aligned as needed.

As PowerSchool pages and functionality are added or removed, the report will be adjusted to reflect all changes.

Estimated Implementation Date: March 2023

Individuals responsible for implementation:

Michelle Thompson, Director I, Enterprise Applications, Technology
Carolyn Moreno, Manager Data Analysis, Enterprise Applications, Technology

Observation 2 - PowerSchool assigns present students the same value as students who have not had their attendance submitted.

Acknowledgement of observation:

- ☒ Agree
☐ Disagree

Management's Response:

PowerSchool provides campus-level staff with a real-time report to identify teachers who have not submitted attendance and extensive training has been provided to campus staff and administration for use of the report. Training included recommendation that the report should be closely monitored, and appropriate action taken daily, prior to the end of the teacher workday. What is missing from the current campus-level report is the inclusion of students associated with the class section that is unsubmitted.

To address this Observation, a PowerSchool campus-level report will be developed by Dallas ISD Information Technology that identifies teachers by section(s) that did not submit daily attendance and lists the students associated with that teacher and section(s). This report will be used by campus administration for assistance with attendance monitoring and reconciliation, if needed.

Training will be provided to campus data controllers, registrars, and administration to run the report prior to the end of each school day to direct teachers to submit attendance and for reconciliation when paper attendance reporting is needed.

Estimated Implementation Date: January 2023

Individuals responsible for implementation:

Michelle Thompson, Director I, Enterprise Applications, Technology

Carolyn Moreno, Manager Data Analysis, Enterprise Applications, Technology

Debra Hill, Director II, Student Data Services, Enterprise Applications, Technology

Observation 3 - Modification controls and edit checks are not implemented for grade calculations and assignments.

Acknowledgement of observation:

☒ Agree

☐ Disagree

Management's Response:

PowerSchool does not have functionality to restrict teachers, in PowerTeacher Pro, from creating their own categories. Teachers are restricted from linking grade weighting of created categories to student overall grade averages. To address this Observation the following processes will be implemented:

- a. A campus-level report will be developed by Dallas ISD Information Technology to identify teacher-created grading categories.
- b. Training will be provided to campus data controllers and administration to run this report weekly and direct the teacher to delete the category prior to end of cycle grade reporting.

Estimated Implementation Date: January 2023

Individuals responsible for implementation:

- a. Michelle Thompson, Director I, Enterprise Applications, Technology

Carolyn Moreno, Manager Data Analysis, Enterprise Applications, Technology

- b. Debra Hill, Director II, Student Data Services, Enterprise Applications, Technology

Observation 4 - Passwords for substitute teachers do not adhere to District policy or best practices.

Acknowledgement of observation:

☒ Agree

☐ Disagree

Management's Response:

Procedural guidance will be provided to school staff, with access to set substitute attendance passwords, to comply with district password best practices. Passwords should be 8 characters or longer, contain at least one of the following: alpha, capital letter, number, and symbol.

Estimated Implementation Date: August 1, 2022

Individuals responsible for implementation:

Debra Hill, Director II, Student Data Services, Enterprise Applications, Technology