



Student Discipline Data Audit

Student Discipline Data Audit

Table of Contents

Executive Summary	3
Background	4
Scope	4
Objective.....	4
Methodology.....	4
Audit Observations and Recommendations	7
Observation 1 – Processes for requesting, permitting, and monitoring manually granted user access should be established.	7
Observation 2 – Audit logs should be utilized to document deleted referrals.	8
Observation 3 – Change management procedures should be established.	9
Conclusion	11
Attachment 1	12
Definition of Risk Level	12
Attachment 2	13
Management Response	13

Date: February 15, 2023

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

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

Subject: Student Discipline Data Audit

Executive Summary

The Dallas Independent School District (District) Office of Internal Audit (OIA) has completed the Student Discipline Data Audit.

The audit focused on the District's internal controls over student discipline data maintained in the Student Positive Behavioral System (SPBS). The audit included reviewing application controls surrounding user access, data accuracy and validity, data backup and recovery, as well as change management controls and record retention efforts 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 within SPBS to mitigate risks such as data security, accuracy, and potential disruptions to district operations. Additionally, Student Engagement and Support (SEAS) has taken a proactive approach to better manage student discipline data by implementing the SPBS system with the assistance of Enterprise Applications.

Opportunities for improvement were identified in the following areas:

1. Processes for requesting, permitting, and monitoring manually granted user access should be established
2. Audit logs should be utilized to document deleted referrals
3. Change management procedures should be established

SPBS maintains sensitive student data. As such, it is important that the data be secured and accurate. One of the most effective and efficient ways to do this is through automating controls by utilizing system implemented controls. If this cannot be done, other manual and monitoring controls should be implemented.

Implementation of the recommendations in this report could assist Enterprise Applications and SEAS in strengthening controls surrounding data maintained within SPBS.

Background

SEAS is responsible for overseeing student disciplinary processes and provides support and resources to school administration to improve educational outcomes. When a student conducts a disciplinary offense, a disciplinary referral is submitted to document the offense and determine what actions are needed. The District offers different remedies such as Disciplinary Alternative Education Programs (DAEP) and Reset Centers to assist educators in addressing student disciplinary matters. Disciplinary referrals and caseloads are managed and tracked in SPBS, which is an Oracle-based online system implemented in the 2021-2022 school year. The system is used to record data such as student offenses, actions taken, conferences that are held, and supporting documentation. In addition, certain student information within SPBS is extracted and provided to the Texas Education Agency (TEA) for PEIMS¹ reporting purposes. There have been approximately 9,000 disciplinary referrals processed in SPBS from August to December 2022. Bullying incidents are managed in a separate system, which was not reviewed as a part of the audit. Enterprise Applications and SEAS are planning to transition management of bullying incidents to SPBS.

Enterprise Applications is responsible for maintaining the system and, in conjunction with SEAS, determines processes surrounding SPBS data management. The main users of the system are campus-based leadership, including principals and assistant principals, SEAS, coordinators at the DAEP schools, and certain members of School Leadership.

Scope

This audit focused primarily on current application controls within SPBS along with related data from fiscal year (FY) 2022-2023 and (FY) 2021-2022.

Objective

The audit objective was to review the District's internal controls over student data maintained within SPBS.

Methodology

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

1. User Access - To determine whether access to student data maintained within SPBS is properly restricted and associated authorizations and privileges are appropriate, auditors performed the following:
 - Auditors attempted to login to SPBS while off the District's network to verify access requires an Enterprise Active Directory (EAD) login and that two-factor authentication was required.No observations were noted.

¹ 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 obtained and reviewed SPBS role-based user authorizations and privileges to determine if appropriate based on job responsibilities and location.
No observations were noted.
 - Auditors obtained a user access listing from SPBS for role-based accounts as of December 20, 2022, totaling 823 users. Of the 823 users, auditors made a statistical sample of 56 users using a 95% confidence level and 5% tolerable deviation rate. For the 56 users sampled, auditors verified they were current employees in Oracle and location and job title matched the allowable access given in SPBS.
No observations were noted.
 - Auditors obtained a user access listing from SPBS for manually granted users as of January 5, 2023, totaling 72 users. Auditors selected all user roles with the classification of assistant principal, central, principal, and school and reviewed the users' job title and location in Oracle to determine if access was appropriate.
See Recommendation 1 in this report.
 - Auditors reviewed system configuration settings to verify users are automatically locked out of the system due to prolonged inactivity.
No observations were noted.
 - Auditors obtained access logs from October 20, 2022, to December 20, 2022, and verified only authorized users accessed the system.
No observations were noted.
2. Data Modifications - To determine if controls are in place to verify modifications to data are appropriately performed, auditors reviewed the system's audit log functions along with SEAS's processes for monitoring high-risk data modifications.
See Recommendation 2 in this report.
 3. Data Accuracy and Validity - To determine if system controls are in place to verify the accuracy and validity of data inputs and outputs, auditors conducted the following:
 - Auditors reviewed a listing of application edit checks in SPBS. Auditors then created referrals in the system's test environment to verify the edit checks were in place and working properly.
No observations were noted.
 - Auditors reviewed data override capabilities within SPBS.
No observations were noted; however, results were communicated to Enterprise Applications and SEAS for review.
 - Auditors requested exceptions reports to review any outliers to system data and determine if they were addressed timely.
No observations were noted.
 4. Data Backup and Recovery - To determine whether there are processes in place to mitigate the potential for significant data loss, auditors reviewed screenshots showing daily automated backups occurred from December 28, 2022, to January 10, 2023. Additionally, auditors

obtained and reviewed the Oracle SaaS Public Cloud Services-Pillar agreement to verify the third-party provider has proper disaster recovery services in place.
No observations were noted.

5. System Administrator Rights - To determine whether administrator rights and privileges are appropriate, auditors conducted the following:

- Auditors obtained a listing of system administrators and reviewed job titles to determine if administrator rights were appropriate based on job function.
No observations were noted.
- Auditors requested procedures for approving, performing, testing, and documenting system changes to determine if proper change management processes are in place.
See Recommendation 3 in this report.

6. Record Retention - To determine if proper record retention processes are in place, auditors reviewed if the system maintains the following to adequately store and retain documents for the required length of time:

- Naming conventions
- Archived document viewing capabilities
- Ability to easily find and access stored documents
- Adequate storage capacity
- Sustainability measures
- Legal hold capabilities

No observations were noted; however, results were communicated to Enterprise Applications and SEAS for 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

Audit Observations and Recommendations

Observation 1 – Processes for requesting, permitting, and monitoring manually granted user access should be established.

Condition

Auditors obtained a user access listing from SPBS for manually granted users, totaling 72 users. Auditors selected all user roles with the classification of assistant principal, central, principal, and school and reviewed to determine if access and associated authorizations and privileges were properly approved and appropriate based on their job function in Oracle. During the review, auditors noted there is no formal process for requesting and documenting manually granted access.

SPBS user access and associated authorizations and privileges are currently granted via different methods. The majority of users are role-based and are granted access to SPBS automatically once their job title is assigned in Oracle. Authorizations for principals and executive directors are role-based, but access is manually managed by School Leadership as executive directors need access to the multiple schools they oversee. Other users who need access for various reasons must be manually granted by SEAS and Enterprise Applications.

Currently, requests for access from non-role-based users are sent informally via phone call or email to SEAS management who then contacts Enterprise Applications to provide access to SPBS. There is no formal process to request access and document the review and approval of manually added users. In addition, there is currently no monitoring process to review manually added users for any needed changes to their access or authorizations that may have resulted from termination, transfer, change in job function, etc.

Criteria

National Institute of Standards and Technology – Security and Privacy Controls for Informational Systems and Organizations, AC-1 Policies and Procedures, September 2020

Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of access control policy and procedures.

National Institute of Standards and Technology – Security and Privacy Controls for Informational Systems and Organizations, AC-2 Account Management, September 2020

Organizations should require approvals by organization-defined personnel for requests to create accounts.

Cause

A formalized process for manually granted user access to SPBS has not been established.

Effect

Lack of processes for determining, documenting, and monitoring user access along with associated authorizations may compromise the security of data maintained in the system. However, auditors noted that SPBS has compensating controls in places such as, all users must have an active EAD account to gain access to the SPBS system; and, therefore, the risk of terminated users having access is mitigated. In addition, the number of manually granted users is limited, further reducing the risk.

Recommendation 1

SEAS and Enterprise Applications should consider developing formal processes and procedures for requesting, approving, documenting, and monitoring manually granted user access. Processes could include use of Laserfiche forms to properly request, review, approve, and document user access. Reports could be periodically generated to review manually granted users on an ongoing basis to adjust for any changes in users or their responsibilities.

Risk Level for Observation 1: Medium²

Observation 2 – Audit logs should be utilized to document deleted referrals.

Condition

Auditors reviewed SPBS audit log features and noted that the system does not currently log deleted referrals. Auditors noted there are some system audit log functions in place, such as for changes made to referral statuses. If a user makes a modification to the status of a referral, such as moving it from “in progress” to “pending completion”, the log records the name of the user who made the change and the date the change occurred. However, if a student referral is deleted, the data is removed from the system, and there is no record that the referral existed or was removed. As there is no record of referral deletions, any removal cannot be properly reviewed for appropriateness.

Criteria

National Institute of Standards and Technology – Security and Privacy Controls for Informational Systems and Organizations, AU-2 Event Logging, September 2020

An event is an observable occurrence in a system. The types of events that require logging are those events that are significant and relevant to the security of systems and the privacy of individuals. Event logging also supports specific monitoring and auditing needs.

Cause

Audit logs currently utilized within SPBS were initiated to address immediate operational needs. A formal process has not yet been conducted to determine where additional audit log functions may be necessary or useful to track significant historical information within SPBS.

² See Attachment 1 for Definition of Risk Level.

Effect

Lack of proper audit logs makes it difficult to validate, verify, and track information. As it relates to record deletion, the inability to determine and review record deletions may result in undocumented student disciplinary events. Additionally, the deletion of student disciplinary referrals could potentially impact PEIMS reporting records. Auditors noted that the likelihood of improper deletion of records is mitigated as authorization to delete referral records is limited to SEAS and those with administrative access.

Recommendation 2

- SEAS and Enterprise Applications should consider utilizing a system audit log function to capture deleted discipline referrals. SEAS should ensure that proper review, approval, and monitoring processes have been established regarding the deletion of student discipline referrals.
- Additionally, SEAS should consider conducting a review to determine where additional audit log functions may be necessary or useful to track significant historical information within SPBS.

Risk Level for Observation 2: Medium³

Observation 3 – Change management procedures should be established.

Condition

Auditors requested change management procedures from Enterprise Applications and noted there are currently no formal change management processes in place for SPBS.

Criteria

National Institute of Standards and Technology – Security and Privacy Controls for Informational Systems and Organizations, CM-3 Configuration Change Control, September 2020

Organizations should document the entire change management process, including authorization.

Cause

A formal change management process was not initially developed for SPBS as Enterprise Applications sought to keep the processes for updating the system as efficient as possible in order to allow for a shorter response time to client requests. However, Enterprise Applications is currently working on developing these processes and procedures

³ See Attachment 1 for Definition of Risk Level.

Effect

Inadequately controlled software libraries increase the risk that unauthorized changes are made to the system and, in this case, student data. In addition, lack of proper controls over modifications to programs could make it difficult to determine which version of the program is the most recent, which can result in inefficiencies and interruptions of service. Lack of processes to properly analyze the effect changes may have and test changes prior to implementation could result in significant impact to security and overall data reliability.

Recommendation 3

Enterprise Applications should consider establishing a formal change management process. The process should consider the following:

- Determine and document the types of changes to the system that are configuration-controlled
- Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses
- Document configuration change decisions associated with the system
- Implement approved configuration-controlled changes to the system
- Retain records of configuration-controlled changes to the system for a time period defined by the organization
- Monitor and review activities associated with configuration-controlled changes to the system
- Coordinate and provide oversight for configuration change control activities through an organization-defined configuration change control element that convenes at an organization-defined frequency when an organization-defined configuration change occurs

Established processes and procedures should be documented and communicated to applicable end-users.

Risk Level for Observation 3: Medium⁴

⁴ See Attachment 1 for Definition of Risk Level.

Conclusion

SPBS is utilized to assist campuses with maintaining an orderly and safe learning environment. As the system houses student data, it is crucial that application controls are implemented to accurately track, monitor, and safeguard student referral data.

Overall, SPBS has controls in place to maintain student discipline data. Implementation of the recommendations in this report could improve the security and reliability of student data along with the performance and functionality of SPBS.

We would like to thank Enterprise Applications and Student Engagement and Support 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., Deputy Superintendent, Chief of Staff and Racial Equity Officer
Sherry West, Deputy Chief, Chief of Staff
Jameile Re'Shad Choice, Executive Director I, Student Discipline, Student Engagement & Support, Chief of Staff
Sean Brinkman, Chief Technology Officer, Information Technology
Roland Antoine, Assistant Superintendent, Enterprise Applications, Information Technology
Matthew Spencer, Director, Enterprise Applications, Information Technology

Acknowledgments:

Eva Narten, CPA, CIA, CISA, Deputy Chief, Internal Audit
Shelly Kelley, CPA, Audit Manager
Sam Willson, CFE, Audit Manager
Claire Chen, CPA, Auditor II
Ashton Loyd, MBA, Auditor I

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 - Processes for requesting, permitting, and monitoring manually granted user access should be established

Acknowledgement of observation:

- ☒ Agree
☐ Disagree

Management's Response:

Enterprise Applications will develop a system that will allow users to request access to the system, this request will require a user from Student Engagement to grant or deny access to that user and what access they should have. Once access is approved, the system will automatically create the user access at the appropriate level. Quarterly, Student Engagement will receive a list of all users who have been granted access for them to audit and verify that they should still have access to the system. Users who no longer need access will be removed. An audit log will exist in the Enterprise Application system to track the creation, update, and deletion of requests

Estimated Implementation Date: May 1, 2023

Individuals responsible for implementation:

Matthew Spencer, Director, Enterprise Applications, Information Technology
Trevis Kaiser, Developer, Enterprise Applications, Information Technology
Michael Johnson, Developer II, Enterprise Applications, Information Technology

Observation 2 – Audit logs should be utilized to document deleted referrals

Acknowledgement of observation:

- ☒ Agree
☐ Disagree

Enterprise Application's Management Response:

Enterprise Applications will add deletion of referrals to the existing audit log and create a page/view for Student Engagement to be able to view pertinent information. If a referral needs to be restored, a service ticket in Service Now will be submitted and the referral will be restored within 2 business days.

Estimated Implementation Date: February 17, 2023

Individuals responsible for implementation:

Matthew Spencer, Director, Enterprise Applications, Information Technology
Trevis Kaiser, Developer, Enterprise Applications, Information Technology

Student Engagement and Support's Management Response:

SEAS will conduct a review to determine where additional audit log functions may be necessary or useful to track significant historical information within SPBS.

Estimated Implementation Date: February 17, 2023

Individuals responsible for implementation:

Jameile Re'Shad Choice, Executive Director I, Student Discipline, Student Engagement & Support, Chief of Staff
Elaine Williams, Director II, Student Engagement & Support, Chief of Staff
Norma Lopez, Coordinator I, Student Engagement & Support, Chief of Staff

Observation 3 – Change management procedures should be established

Acknowledgement of observation:

- ☒ Agree
- ☐ Disagree

Management's Response:

Enterprise Applications will follow existing IT SOPs regarding change management and control. Changes will be submitted to Change Advisory Board for approval before they are made.

Estimated Implementation Date: Immediate

Individuals responsible for implementation:

Matthew Spencer, Director, Enterprise Applications, Information Technology
Trevis Kaiser, Developer, Enterprise Applications, Information Technology