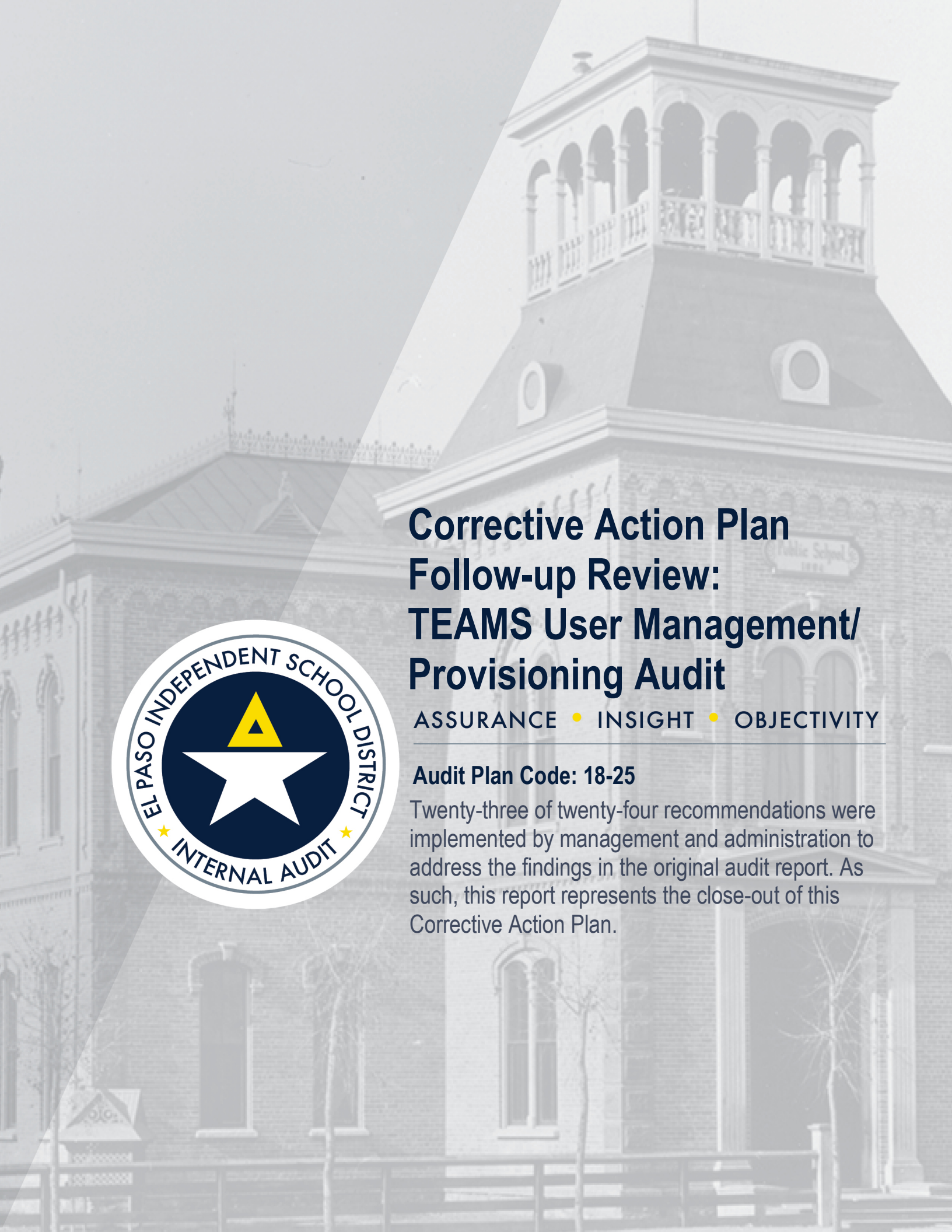

Corrective Action Plan Follow-up Review: TEAMS User Management/ Provisioning Audit

ASSURANCE • INSIGHT • OBJECTIVITY

Audit Plan Code: 18-25

Twenty-three of twenty-four recommendations were implemented by management and administration to address the findings in the original audit report. As such, this report represents the close-out of this Corrective Action Plan.

Contents

ASSURANCE • INSIGHT • OBJECTIVITY

Follow-up Review

Abbreviations

CAP	Corrective Action Plan
IA	Internal Audit
ISO	International Organization for Standardization (an information security framework)
TS	Technology Services
HR	Human Resources
TEAMS	Total Education Administrative Management Solution
CAP	Corrective Action Plan

Follow-up Review

ASSURANCE • INSIGHT • OBJECTIVITY

Background

As part of the reporting and audit process, the Institute of Internal Auditors' (IIA) International Standards for the Professional Practice of Internal Auditing, Performance Standard 2500 - Monitoring Progress, require we "…establish and maintain a system to monitor the disposition of results communicated to management." In order to comply with this standard, we performed this corrective action plan follow-up review to monitor the status of the recommendations referenced in the original audit report.

Internal Audit issued the TEAMS User Access Management/Provisioning Audit Report to District management and administration on May 11, 2016. We performed the audit as part of the Board approved 2015-2016 Internal Audit Plan. The objective of the audit was to provide assurance that controls were in place and working as intended to ensure user access administration/provisioning is managed and monitored, including controls over privileged access (i.e. super users) for the Total Education Administrative Management (TEAMS) modules. We found significant deficiencies in the design and operation of Technology Services' user access controls, including controls over privilege access (i.e. super users), exposing the District to risks of inappropriate and/or unauthorized access/activities within TEAMS. The original audit report included nine (9) findings, one (1) observation, and 24 recommendations to mitigate the risks identified. District management and administration agreed with our recommendations and developed a corrective action plan (CAP) with 21 activities. For reference, a Summary of the Original Audit Report Findings is shown as **Exhibit A**.

Objective and Scope

The objective and scope of this follow-up review was limited to determining whether management and administration implemented the 24 recommendations outlined in the 21 CAP activities or took other actions to address the nine (9) findings and one (1) observation referenced in the original TEAMS User Access Management/ Provisioning Audit Report.

Methodology

To achieve our follow-up review objective, we:

- Held meetings and communicated with persons responsible for carrying out the CAP activities.
- Reviewed supporting documentation maintained by management as evidence of completion of the CAP activities provided to Internal Audit.

Inherent Limitations

This was a limited scope follow-up review covering only the actions taken by administration to address the original audit findings and recommendations stated in the Objective and Scope section of this report. No representations of assurance are made to other areas or periods not covered by this follow-up review.

Summary of Results

Management and administration developed a total of 21 corrective action activities to address the 24 recommendations as shown below:

Recommendations	Implemented	Overall CAP Status
24	23*	Closed

*The recommendation not implemented was an alternative to a separate recommendation that was implemented; it was not necessary to implement both recommendations. See recommendation nine (9).

This report represents the close-out of this corrective action plan (CAP) based on our review of evidence.

Original Recommendations and Status of CAP Activities

The original recommendations, the CAP activities (response from management/administration), person(s) responsible, and the status of the CAP activities are outlined below. Please note that CAP activities one (1) to two (2) were administrative requirements when completing and submitting the CAP itself; therefore, the CAP activities below do not reference these two CAP activities.

1

Original Recommendation: Technology Services (TS) should perform an inventory of all super user accounts and properly authorize them using the "principle of least privilege".

Management and Leadership Response: Agreed with recommendation and incorporated into the CAP as activity four (4) as follows:

Activity 4: "Technology Services will inventory and audit using the principal of least privilege for employees with super user access to job role and function. Approval to be granted by Chief Information Officer and Deputy Superintendent of Finance and Operations."

Person Responsible: Director Application Services, Technology Services

Status: Implemented

2

Original Recommendation: All super users should be fingerprinted and background check results be reviewed by Human Resources (HR) and TS leadership.

Management and Leadership Response: Agreed with recommendation and incorporated into the CAP as activity five (5) as follows:

Activity 5: "HR will administer the finger print requirement for all super users and report findings to Chief Technology Officer, Technology Services. Any findings of unethical behavior will be addressed by HR and TS leadership to determine appropriate action(s)."

Persons Responsible: Assistant Superintendent Human Resources; Chief Technology Officer, Technology Services; and Director Administrative Services, Technology Services

Status: Implemented

3 **Original Recommendation**: The District should consider establishing non-disclosure and/or confidentiality affidavits for super users.

Management and Leadership Response: Agreed with recommendation and incorporated into the CAP as activity six (6) as follows:

Activity 6: "All TS staff will sign and adhere to a non-disclosure and/or confidentiality affidavit. This process will repeat itself at the beginning of each fiscal year."

Persons Responsible: Chief Information Officer, Technology Services; Director Applications, Technology Services; and Information Security Officer, Technology Services

Status: Implemented

4 **Original Recommendation**: The District should consider requiring separate accounts be created for each super user, one for system administration job responsibilities and the other for the day-to-day normal user account job responsibilities.

Management and Leadership Response: Agreed with recommendation and incorporated into the CAP as activity seven (7) as follows:

Activity 7: "Establish separate user accounts for all super users to perform day to day activities at a non-privileged level. Each user will have a unique user ID to maintain accountability for each access attempt."

Persons Responsible: Chief Information Officer, Technology Services; Director Applications, Technology Services; and Information Security Officer, Technology Services

Status: Implemented

5 **Original Recommendation**: Super user activity should be logged. Their activity should be reviewed on a periodic basis by a party independent of the Technology Services - Administrative Services staff.

Management and Leadership Response: Agreed with recommendation and incorporated into the CAP as activity eight (8) as follows:

Activity 8: "TS will audit superuser access to TEAMS database."

Persons Responsible: Chief Information Officer, Technology Services; Director Applications, Technology Services; and Information Security Officer, Technology Services

Status: Implemented

6 **Original Recommendation**: Technology Services leadership should review each super users' access needs on a periodic basis to determine if such access is still needed.

Management and Leadership Response: Agreed with recommendation and incorporated into the CAP as activity nine (9) as follows:

Activity 9: "TS leadership will review super user access on a semiannual basis and adjust privileges as needed."

Persons Responsible: Chief Information Officer, Technology Services; Director Applications, Technology Services; and Information Security Officer, Technology Services

Status: Implemented

7 **Original Recommendation**: Technology Services leadership should establish formal processes to remove access from individuals with super user access in the most efficient and timely manner.

Management and Leadership Response: Agreed with recommendation and incorporated into the CAP as activities nine (9) and 21 as follows:

Activity 9: "TS leadership will review superuser access on a semiannual basis and adjust privileges as needed."

Activity 21: "TS will develop written access control procedures based on Board policy CQ (Regulation) that includes requirements for activities outlined in this CAP and review annually."

Persons Responsible: Chief Information Officer, Technology Services; Director Applications, Technology Services; and Information Security Officer, Technology Services

Status: Implemented

8 **Original Recommendation**: Technology Services should confirm with the developer of DbVisualizer if it is possible for it to generate user activity logs for changes made directly to the TEAMS database.

Management and Leadership Response: Agreed with recommendation and incorporated into the CAP as activity eight (8) as follows:

Activity 8: "TS will audit superuser access to TEAMS database."

Persons Responsible: Chief Information Officer, Technology Services; Director Applications, Technology Services; and Information Security Officer, Technology Services

Status: Implemented

9 **Original Recommendation**: If recommendation eight (8) is not feasible, a manual "check-out" process should be implemented for the DbVisualizer full-access account. When a change to the TEAMS database is planned using DbVisualizer the full-access account should be checked out from an employee with no access to DbVisualizer. These changes should be documented with evidence of who made change, date, purpose, outcome, and signature of second person attesting to the change. Documentation should be archived.

Management and Leadership Response: As recommendation eight (8) was feasible, it was not necessary to establish a CAP activity to address recommendation nine (9).

Status: Not Implemented

10 **Original Recommendation**: Technology Services leadership should establish a strong "tone at the top" culture in its control environment to communicate its commitment to internal controls.

Management and Leadership Response: Agreed with recommendation and incorporated into the CAP as activity 10 as follows:

Activity 10: "TS management will clearly communicate its ethics and values to department staff on annual basis to establish a "strong tone at the top" culture.

Establish a streamline process to avoid overrides and if needed, limit them to extreme or extenuating circumstances and always fully documented"

Persons Responsible: Chief Information Officer, Technology Services; Director Applications, Technology Services; and Information Security Officer, Technology Services

Status: Implemented

11 **Original Recommendation**: All TS employees (data custodians) should go through the same user access authorization process as all other District employees.

Management and Leadership Response: Agreed with recommendation and incorporated into the CAP as activity 11 as follows:

Activity 11: "Data owners will approve current TS staff access to their TEAMS system modules. TS Staff will only receive access to TEAMS modules for which they support. Special approval from data owners will be required if special access is needed to accomplish a task, and for what period of time."

Persons Responsible: Director Applications, Technology Services.

Status: Implemented

12 **Original Recommendation**: Technology Services and data owners should determine which TEAMS' access requires authorization from data owners in addition to authorization from the budget authority, before granting access.

Management and Leadership Response: Agreed with recommendation and incorporated into the CAP as activity 12 as follows:

Activity 12: "TS and data owners will determine which TEAMS access requires authorization outside of the role-based access defaults. These elevated access rights will be the ones data owners will need to approve on a case by case basis."

Persons Responsible: Chief Information Officer, Technology Services; Director Applications, Technology Services; and Information Security Officer, Technology Services

Status: Implemented

13 **Original Recommendation**: Technology Services should standardize access privileges of roles with the same/similar responsibilities, this will result in limiting the number of roles with different system privileges.

Management and Leadership Response: Agreed with recommendation and incorporated into the CAP as activity 13 as follows:

Activity 13: "TS and data owners will determine what access each job role should have, using the principle of least privileged."

Person Responsible: Director Administrative Services, Technology Services

Status: Implemented

14 **Original Recommendation**: Technology Services should work with administration and data owners to review and determine the access privileges that each role/position should have using the "principle of least privilege".

Management and Leadership Response: Agreed with recommendation and incorporated into the CAP as activities three (3) and 13 as follows:

Activity 3: "TS will present CAP to Executive Cabinet to obtain commitment from stakeholders."

Activity 13: "TS and data owners will determine what access each job role should have, using the principle of least privileged."

Persons Responsible: Chief Technology Officer and Director Administrative Services, Technology Services

Status: Implemented

15

Original Recommendation: Technology Services should implement an automated access request workflow solution. To increase the effectiveness and efficiency in the user access authorization process, the design of this solution should have internal controls in place which documents all phases of the process.

Management and Leadership Response: Agreed with recommendation and incorporated into the CAP as activity 14 as follows:

Activity 14: "TS will develop an access request process with data owner approval. Will consult with IA to establish an online automated process."

Person Responsible: Director Applications, Technology Services

Status: Implemented

16

Original Recommendation: Technology Services, as the data custodians, should meet with data owners to formalize and document the user access review process for the TEAMS modules.

Management and Leadership Response: Agreed with recommendation and incorporated into the CAP as activity 15 as follows:

Activity 15: "TS will conduct a meeting with data owners to formalize and document the user access review process. TS will develop reports/views of user access. Each data owner will review information from the views of user access and request access changes (if necessary) on a periodic basis. Risk assessment will be addressed for users with access to highly sensitive HR information may be performed at more frequent intervals."

Person Responsible: Information Security Officer, Technology Services

Status: Implemented

17

Original Recommendation: Technology Services should ensure an initial full user access review and subsequent reviews be based on a risk assessment. This process should be based on the framework (ISO 27001 and best practices covered in ISO 27002) used by TS leadership to develop the District's information security policy.

Original Observation: Technology Services should work with the Assistant Superintendent of HR or designee to perform a user access review of all positions with access to the TEAMS HR module containing electronic personnel files. Also, in the future, all user requests for access to the TEAMS HR module containing the electronic personnel file be approved/authorized by the Assistant Superintendent of HR or designee.

Management and Leadership Response: Agreed with recommendation and incorporated into the CAP as activity 15 as follows:

Activity 15: "TS will conduct a meeting with data owners to formalize and document the user access review process. TS will develop reports/views of user access. Each data owner will

review information from the views of user access and request access changes (if necessary) on a periodic basis. Risk assessment will be addressed for users with access to highly sensitive HR information may be performed at more frequent intervals."

Person Responsible: Information Security Officer, Technology Services

Status: Implemented

18 **Original Recommendation**: Technology Services should remove TEAMS access from substitute and temporary employees after a specified period of time when they are not in an active work assignment. This time period should be determined by each data owner.

Management and Leadership Response: Agreed with recommendation and incorporated into the CAP as activity 16 as follows:

Activity 16: "The issue of removing TEAMS access from substitute and temporary employees is currently being addressed by HR, Finance and TS staff."

Person Responsible: Director Administrative Services, Technology Services, and Assistant Superintendent Human Resources

Status: Implemented

19 **Original Recommendation**: Mitigating controls should be designed and implemented to ensure Prologic's superuser account is properly authorized, managed, and monitored as all other District TEAMS super users.

Management and Leadership Response: Agreed with recommendation and incorporated into the CAP as activities eight (8), 11, and 12 as follows:

Activity 8: "TS will audit superuser access to TEAMS database."

Activity 11: "Data owners will approve current TS staff access to their TEAMS system modules. TS staff will only receive access to TEAMS modules for which they support. Special approval from data owners will be required if special access is needed to accomplish a task, and for what period of time."

Activity 12: "TS and data owners will determine which TEAMS access requires authorization outside of the role-based access defaults. These elevated access rights will be the ones data owners will need to approve on a case by case basis."

Persons Responsible: Chief Information Officer, Technology Services; Director Applications, Technology Services; and Information Security Officer, Technology Services

Status: Implemented

20 **Original Recommendation**: Technology Services should consult with the District's General Counsel to review the current Prologic agreement (dated 2007), keeping the District's information security controls in mind as it relates to Prologic's access to TEAMS and related database(s).

Management and Leadership Response: Agreed with recommendation and incorporated into the CAP as activities 17 and 18 as follows:

Activity 17: "TS to develop a Document of Understanding between EPISD and Prologic, based upon legal counsel review. The DOU will address Prologic access to District data and understanding that the District will be the only entity to operate the database. This document will be legally binding."

Activity 18: "TS will ensure that Prologic is aware of and compliant with the District's information security policies and procedures. Acknowledgements of compliance with the District's information security policy will be included in the DOU and reviewed annually to coincide with annual maintenance and support requisition process."

Persons Responsible: Chief Information Officer, Technology Services; Director Applications, Technology Services; Information Security Officer, Technology Services; and Legal Counsel

Status: Implemented

21 **Original Recommendation**: Appropriate written procedures around data classification should be developed and adopted to support the District's information security policy. These procedures should be based on the framework (ISO 27001 and best practices covered in ISO 27002) used by TS leadership to develop the District's information security policy (CQ Regulation).

Management and Leadership Response: Agreed with recommendation and incorporated into the CAP as activity 19 as follows:

Activity 19: "TS will develop a data classification policy. The policy will specify classifications as well as commensurate access procedures."

Persons Responsible: Information Security Officer, Technology Services

Status: Implemented

22 **Original Recommendation**: The data classification standard operating procedures should be reviewed by TS leadership on a periodic basis.

Management and Leadership Response: Agreed with recommendation and incorporated into the CAP as activity 20 as follows:

Activity 20: "TS will review classification policy and standard operating procedures annually."

Persons Responsible: Chief Information Officer, Technology Services; Director Applications, Technology Services; and Information Security Officer, Technology Services

Status: Implemented

23 **Original Recommendation**: Appropriate written procedures around access control should be developed and adopted to support the District's information security policy. We recommend these procedures be based on the framework (ISO 27001 and best practices covered in ISO 27002) used by TS leadership to develop the District's information security policy.

Management and Leadership Response: Agreed with recommendation and incorporated into the CAP as activity 21 as follows:

Activity 21: "TS will develop written access control procedures based on Board policy CQ (Regulation) that includes requirements for activities outlined in this CAP and review annually."

Persons Responsible: Chief Information Officer, Technology Services; Director Applications, Technology Services; and Information Security Officer, Technology Services

Status: Implemented

24 **Original Recommendation**: The access control standard operating procedures should cover controls around privileged access (i.e. super users) and be reviewed by TS leadership on a periodic basis.

Management and Leadership Response: Agreed with recommendation and incorporated into the CAP as activity 21 as follows:

Activity 21: "TS will develop written access control procedures based on Board policy CQ (Regulation) that includes requirements for activities outlined in this CAP and review annually."

Persons Responsible: Chief Information Officer, Technology Services; Director Applications, Technology Services; and Information Security Officer, Technology Services

Exhibit A – Summary of Original Audit Report Findings

Finding	Summary Finding
A	**Super user access to TEAMS and DbVisualizer (a third-party database management tool):** Mitigating controls are not in place to ensure super users are properly authorized, managed, and monitored to limit/minimize the risk of inappropriate access/activities. Super users represent one of the most significant risks, from an access governance point of view, to organizations as they have unlimited access (including the ability to add, edit, and delete) to all system resources. *TEAMS* Based on information provided by TS, five TEAMS users labeled as super users were identified. However, we were notified about the existence of other accounts with super user access privileges not included in the information provided for this audit. As such, it is likely there are other TEAMS users with super user access privileges not labeled as super users. *DbVisualizer* Technology Services identified 12 additional users with access to one shared DbVisualizer full-access account; these accounts have similar access privileges as super users.
B	**Granting Access - Proper authorization to access TEAMS:** 1. We found evidence that shows an attempt by TS leadership to override a user access granting control. Overrides of internal controls may be acceptable under extenuating circumstances. However, information provided by TS did not support that an extenuating circumstance was the reason for the attempt to override a user access granting control. Internal controls apply to all District employees regardless of level/title. 2. We tested 40 user access requests and found the following: • Six user access requests had unreliable evidence of authorization from budget authority, and • Two user access requests did not have documented evidence of authorization from budget authority.
C	**Periodic reviews on who has access to TEAMS modules:** User access reviews, for the TEAMS modules, have not been performed as required by the information security policy (Board Policy CQ Regulation) developed by Technology Services in 2013. The policy requires user access reviews be performed by Management at regular intervals using a formal process. Over the years some positions may have accumulated privileges they may or may no longer need to perform their job responsibilities. As such, there is an increased: • Risk of inappropriate/unauthorized access by users who do not need such access to perform their job responsibilities, • Risk of unauthorized access by separated employees, • Reputational, operational, and financial risk to the District if data access is abused and/or data is breached, whether intentional or accidental.
D	**Removing access – Prompt removal of access to TEAMS:** No significant reportable findings related to removing access were noted from our sample of 40 users who have separated (or left) the District. However, during our completeness and accuracy test for this area, we found one temporary employee's access was not removed for at least three months after the employee resigned.
E	**Third-Party Access Controls:**

Finding	Summary Finding
	1. Mitigating controls are not in place to ensure Prologic's (developer/creator of TEAMS) super user access to the District's data is properly authorized, managed, and monitored to limit/minimize the risk of inappropriate access/activities. 2. The contract with Prologic (dated 2007) does not define or include the District's information security requirements the vendor must abide by when managing, accessing, handling or otherwise interacting with the District's TEAMS data.
F	**<u>Data Classification – Classifying data according to its value and/or importance:</u>** Written standard operating procedures do not exist for data classification required under the District's information security policy (Board Policy CQ Regulation). Data classification is a major part of the user access management process because it defines: the value and/or importance of the data to the organization, the data owner(s), the person(s) responsible for approving user access privileges and access levels, and the extent and depth of security controls. The absence of data classification standard operating procedures increases the risk of: • Inappropriate/unauthorized access to the TEAMS system, including access to sensitive and/or confidential information, • Sensitive and highly confidential data not having the correct level of protection, • Privacy, data confidentiality, and integrity incidents, • Security roles created by TS not having the appropriate security level against accessing private and/or highly confidential information, • Serious non-compliance with federal (HIPPA, FERPA), state laws, and local policy requirements.
G	**<u>Access Control - Requirements that specify how access is managed and who may access information under what circumstances:</u>** Formal written standard operating procedures do not exist specifying how access controls will be followed/performed in actual practice as required by the District's information security policy (Board Policy CQ Regulation). Rather, informal and unwritten processes are in place to manage user access in the TEAMS system. As a result, there is an increased risk of inappropriate/unauthorized access to the TEAMS system, including access to sensitive and/ or confidential information found in the TEAMS modules.
Observation	Technology Services should work with the Assistant Superintendent of HR or designee to perform a user access review of all positions with access to the TEAMS HR module containing electronic personnel files. Also, in the future, all user requests for access to the TEAMS HR module containing the electronic personnel file be approved/authorized by the Assistant Superintendent of HR or designee.

EL PASO INDEPENDENT SCHOOL DISTRICT

BOARD OF TRUSTEES

Trent Hatch, Board President
Bob Geske, Vice President
Al Velarde, Secretary
Susie Byrd
Diane Dye
Mickey Loweree
Chuck Taylor

EPISD Internal Audit Department
6531 Boeing Drive. El Paso, TX 79925
Phone 915-230-2740 Email audit@episd.org

Fraud, Waste, and Abuse Hotline:
https://www.reportlineweb.com/EPISD or 800-620-8591

YouTube EPISD.org