Internal Audit Department

Report to Board of Trustees and Administration

2015-2016

TEAMS USER ACCESS MANAGEMENT/ PROVISIONING AUDIT

Significant deficiencies exist in the design and operation of Technology Services' user access controls, including controls over privileged access (i.e. super users), exposing the District to risks of inappropriate and/or unauthorized access/activities within TEAMS.

Audit Plan Code: 16-07/16-15

Contents

Abbreviations and Definitions

Abbreviations List

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

Definitions

Access Control*	"The processes, rules and deployment mechanisms that control access to information systems, resources and physical access to premises."
Budget Authority	An employee, normally a director or above, responsible for the administration of budgeted funds for their campus/department or operating unit. In terms of their role in user access management/provisioning, they currently review, approve, and/or deny access requests for employees under their supervision.
Data Owner*	"The individual(s), normally a manager or director, who has the responsibility for the integrity, accurate reporting and use of computerized data." For example, the data owner of the TEAMS HR module data is the Assistant Superintendent of Human Resources.
Data Custodian*	"The individual(s) and department(s) responsible for the storage and safeguarding of the computerized data." For example, the data custodian of the data residing in the TEAMS modules is Technology Services (TS).
Data Classification*	"The assignment of a level of sensitivity to data (or information) that results in the specification of controls for each level of classification. Levels of sensitivity of data are assigned according to predefined categories as data are created, amended, enhanced, stored, or transmitted. The classification level is an indication of the value or importance of the data to the enterprise."
DbVisualizer (DbVis)	A third-party database management tool used by TS to run queries and to make significant/mass changes on the Total Education Administrative Management Solution (TEAMS) database.
Full-access DbVisualizer Account	A DbVisualizer account with access to make changes to the TEAMS database.
ISO 27001/27002	An information security framework and best practices published by the International Organization for Standardization. Technology Services' leadership used ISO 27001 to develop the District's information security policy.
Mitigating Controls	Controls that reduce the potential impact should an event occur. For example, the TS leadership may put in place a control to log and review certain user activity to detect inappropriate/unauthorized user activities.

Principle of Least Privilege*	"Controls used to allow the least privilege access needed to complete a task." For example, a teacher may not need access to the TEAMS HR module to perform his/her job.
Prologic Technology Systems (Prologic)	Third party developer/creator of TEAMS.
Risk Assessment	"A process used to identify and evaluate risk and its potential effects."
TEAMS Super User Account	A TEAMS account with unlimited access (including the ability to add, edit, and delete) to all TEAMS system resources. Such accounts are necessary to administer and maintain the TEAMS system.
Total Education Administrative Management Solution (TEAMS)	An enterprise resource planning software with different modules (such as HR, Accounting, Student, etc.) within a single shared database.
User Access Review	A periodic review of system users' access performed by data (business) owners. "This review, while facilitated by the IT Department, should be conducted by the organization with approvals received from each responsible business owner." (The Institute of Internal Auditors – GTAG Identity and Access Management Practice Guide)

* As defined by the Information Systems Audit and Control Association (ISACA) 2015 Glossary of Terms

Internal Audit Report

Background

This audit is part of the Board approved 2015-2016 Internal Audit Plan and was identified as a high risk area during the Risk Assessment and as an area of concern by Internal Audit staff.

Objective and Scope

The objective was to provide assurance that controls are 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 Solution (TEAMS) modules.

The scope of the audit included reviewing policies in place, evaluating controls around granting, reviewing, and revoking TEAMS access, including controls over super users for the July 1, 2014 to February 15, 2015 period.

Methodology

In order to achieve the audit objective we:

- Researched relevant Board policies, International Organization for Standardization (ISO) 27001/27002, and information security best practices,
- Reviewed written standard operating procedures (if in place) and determined if they were consistent with industry standards and best practices,
- Sent internal control questionnaires and performed process walkthroughs,
- Performed user access tests on a sample basis,
- Obtained a snapshot (at a point in time), reviewed, and summarized all positions with access to highly confidential Human Resources (HR) information.

We believe the evidence obtained is sufficient to support our findings and conclusions to meet the audit objective.

Limitations

In accordance with the *Institute of Internal Auditors' Practice Advisory 2320-3: Audit Sampling*, "The internal auditor should validate the completeness of the population to ensure that the sample is selected from an appropriate data set." As the objective of this audit did not include testing all Information Technology General Controls over applications that produce the system generated data/reports we used to select our sample selections from, we performed manual completeness and accuracy validation checks.

These sample accuracy validation checks gave us a limited level of confidence on the completeness of the TEAMS data provided by Technology Services (TS) for our testing purposes. Therefore, we cannot ascertain populations provided from TEAMS by TS were 100% complete and accurate.

Some of the evidence and parameters used to identify and test processes and controls in place, was based on inquiry due to limited availability of related written procedures. To lessen the

effect of this limitation, we corroborated parameters used in our testwork with the information security framework (ISO 27001) used by TS and information security best practices.

Findings and Recommendations (A to G)

A. <u>Super user access to TEAMS and DbVisualizer (a third-party database management tool):</u>

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.

Recommendations:

Mitigating controls should be designed and implemented to ensure super users are properly authorized, managed, and monitored, such as:

1. Technology Services should perform an inventory of all super user accounts and properly authorize them using the "principle of least privilege".
2. All super users should be fingerprinted and background check results be reviewed by HR and TS leadership.
3. The District should consider establishing non-disclosure and/or confidentiality affidavits for super users.
4. 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.
5. 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.
6. Technology Services leadership should review each super users' access needs on a periodic basis to determine if such access is still needed.
7. Technology Services leadership should establish formal processes to remove access from individuals with super user access in the most efficient and timely manner.
8. 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.
9. If recommendation 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.

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.

Recommendations:

1. Technology Services leadership should establish a strong "tone at the top" culture in its control environment to communicate its commitment to internal controls.
2. All TS employees (data custodians) should go through the same user access authorization process as all other District employees.
3. 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.
4. 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.
5. 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."
6. 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.

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.

Recommendations:

1. Technology Services, as the data custodians, should meet with data owners to formalize and document the user access review process for the TEAMS modules.
2. 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.

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.

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.

E. Third-Party Access Controls:

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.

Recommendations:

1. Mitigating controls should be designed and implemented to ensure Prologic's super user account is properly authorized, managed, and monitored as all other District TEAMS super users.
2. 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).

F. Data Classification – Classifying data according to its value and/or importance

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.

Recommendations:

1. 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).

2. The data classification standard operating procedures should be reviewed by TS leadership on a periodic basis.

G. Access Control - Requirements that specify how access is managed and who may access information under what circumstances:

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.

Recommendations:

1. 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.
2. 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.

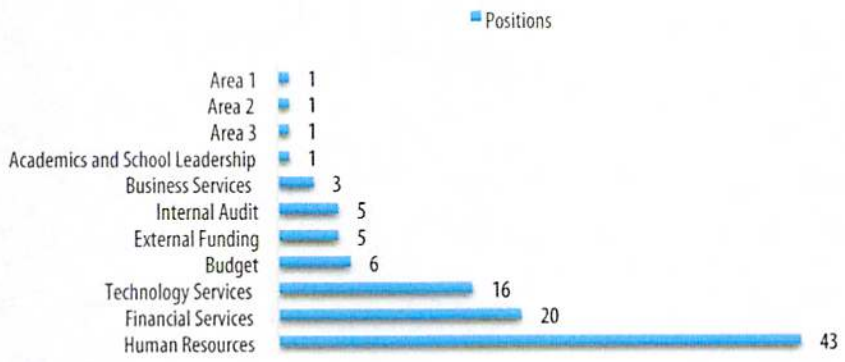
Observation

While conducting this audit an observation was made that was outside of our original scope and objective. We identified 102 positions with access to, at a minimum, view the contents of the TEAMS Human Resources (HR) module. The HR module contains the electronic version of employees' personnel files, which include highly sensitive and confidential employee information. Fifty-nine (59) or approximately 58% of these positions reside outside of the HR department; these positions may not have a business need to view such information. ***See Figure 1*** which shows departments and positions with access to electronic HR personnel files.

Recommendations:

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.

Figure 1: Positions with access to electronic HR personnel files by department



Analysis of Corrective Action Plan from Management

A corrective action plan (CAP) was provided outlining the activities to be implemented. The CAP appears to be sufficient to address the findings/concerns delineated in the report. However, CAP activities did not specify (i) how TS will implement independent reviews of super user activity and (ii) the frequency TS will be communicating ethics and code of conduct to its employees. As such, we will closely monitor how these specific items are addressed as part of our follow-up on the implementation of the CAP.

Conclusion

As it relates to TEAMS user access controls, the TS Department has not formally assessed relevant information security risks. As a result, we found significant deficiencies in the design (i.e. implementation) and operation of TS' user access controls, including controls over privileged access (i.e. super users), exposing the District to risks of inappropriate and/or unauthorized access/activities within TEAMS. It is important to note user access controls are imperative in TEAMS and other software systems used by the District.

Furthermore, the TS department's internal control environment should be strengthened by TS leadership by establishing a strong "tone at the top" culture to communicate its positive commitment to internal controls. The control environment sets the tone of a department/organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. If the tone set by leadership supports internal controls, employees will be more inclined to support internal controls and uphold the same values. However, if leadership appears unconcerned with internal controls, employees will be more prone to override controls, because they feel that internal controls are not a focus or priority within the department/organization.

We believe the implementation of a corrective action plan to address the findings is critical to support:

1. Technology Services Mission to provide: "Efficient & effective business practices" and "data compliance" services to the District.

2. District's Improvement Plan Goal 3 which states: "El Paso ISD will demonstrate fiscal and ethical responsibility as well as a deep commitment to service orientation in all district operations." Along with related Performance Objective 1 which states: "Develop adequate planning processes, plans, implementation strategies, action steps and communication protocols to guide district initiatives, program direction and system operations."

Exhibit A: Criteria Table.

Criteria No.		Criteria Source	Criteria Details
1		**Board Policy CQ (Regulation), Technology Resources - ISO 27001 Objectives and Controls:**	"Technology services will follow industry standard ISO 27001, which specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving documented information security management system."
2		**Board Policy CQ (Regulation), Technology Resources - User Access Management Section:**	"To ensure authorized user access and to prevent unauthorized access to information systems: 1. There will be a formal user registration and deregistration procedure in place for granting and revoking access to all information systems and services. 2. The allocation and use of privileges will be restricted and controlled. 3. The allocation of passwords will be controlled through a formal management process. 4. Management will review users' access rights at regular intervals using a formal process."
3		**Board Policy CQ (Regulation), Technology Resources - Monitoring Section:**	"- Audit logs recording user activities, exceptions, and information security events will be produced and kept for an agreed period to assist in future investigations and access control monitoring. - Procedures for monitoring use of information processing facilities will be established and the results of the monitoring activities reviewed regularly. - System administrator and system operator activities will be logged."
4	*	**ISO 27001 Control A.9.2.3 - Management of privileged access rights:**	"The allocation and use of privileged access rights should be restricted and controlled."
5	*	**ISO 27001 Control A.9.2.1 - User registration and de-registration:**	"A formal user registration and de-registration process should be implemented to enable assignment of access rights."
6	*	**ISO 27001 Control A.9.2.2 - User access provisioning:**	"A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services."
7	*	**ISO 27001 Control A.9.2.5 - Review of user access rights:**	"Asset owners should review users' access rights at regular intervals."
8		**Institute of Internal Auditors: Global Technology Audit Guide - Identity and Access Management - Periodic Monitoring of Access Rights:**	"...the organization should establish a methodology to periodically review the access rights granted to all identities residing in its IT environment. This review, while facilitated by the IT department should be conducted primarily by the organization with approvals received from each responsible business owner. In addition, privileged and IT account identities should be reviewed by an appropriate manager or system owner."
9	*	**ISO 27001 A.9.2.6 - Removal or adjustment of access rights:**	"The access rights of *all employees* and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change."
10		**Board Policy CQ (Regulation), Technology Resources - Termination / Revocation of System User Account:**	"*Termination of an employee's* or a student's access for violation of District policies or regulations will be *effective on the date* the principal or District coordinator receives notice of student withdrawal or of revocation of system privileges, or on a future date if so specified in the notice."

Exhibit A: Criteria Table.

Criteria No.		Criteria Source	Criteria Details
11		**Board Policy CQ (Regulation), Technology Resources - External Parties:**	"To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties: 1. The risks to the organization's information and information processing facilities from business processes involving external parties will be identified and appropriate controls implemented before granting access. 2. All identified security requirements will be addressed before giving customers access to the organization's information or assets. 3. Agreements with third parties involving accessing, processing, communicating, or managing the organization's information or information processing facilities, or adding products or services to information processing facilities will cover all relevant security requirements."
12		**Board Policy CQ (Regulation), Technology Resources - External Parties:**	"To implement and maintain the appropriate level of information security and service delivery in line with third-party service delivery agreements: 1. It will be ensured that the security controls, service definitions, and delivery levels included in the third-party service delivery agreement are implemented, operated, and maintained by the third party. 2. The services, reports, and records provided by the third party will be regularly monitored and reviewed, and audits will be carried out regularly. 3. Changes to the provision of services, including maintaining and improving existing information security policies, procedures, and controls, will be managed, taking account of the criticality of business systems and processes involved and reassessment of risks."
13		**Board Policy CQ (Regulation), Technology Resources - Monitoring:**	"To detect unauthorized information processing activities: 1. Audit logs recording user activities, exceptions, and information security events will be produced and kept for an agreed period to assist in future investigations and access control monitoring. 2. Procedures for monitoring use of information processing facilities will be established and the results of the monitoring activities reviewed regularly. 3. Logging facilities and log information will be protected against tampering and unauthorized access. 4. System administrator and system operator activities will be logged. 5. Faults will be logged, analyzed, and appropriate action taken. 6. The clocks of all relevant information processing systems within an organization or security domain will be synchronized with an agreed accurate time source."