Audit Plan Code: 17-03

CAMPUS ACCOUNTING SYSTEM CONVERSION CONSULTING ENGAGEMENT

Recommendations based on best practices included

EL PASO INDEPENDENT SCHOOL DISTRICT

Internal Audit Department

Contents

ABBREVIATIONS LIST

CA	Campus Accounting
CAM	Campus Accounting Manual
CAP	Corrective Action Plan
FY	Fiscal Year
IA	Internal Audit
ISO	Information Security Officer
SFO	School Funds Online
TRA	Technology Resource Associates

Consulting Engagement Report

Introduction

Consulting engagements are advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and improve the District's governance, risk management, and control processes. According to the Institute of Internal Auditors' Standards, "…When performing consulting services the internal auditor should maintain objectivity and not assume management responsibility." As such, throughout the consulting engagement we may make recommendations to the process owner to minimize risks or increase efficiencies, but the process owner is ultimately responsible for making decisions on implementing recommendations made. If the process owner accepts a level of risk that may be unacceptable to the District, the Chief Internal Auditor must discuss the matter with cabinet level administration and to the Board if the matter has not been resolved.

The consulting engagement did not include an audit of the campus accounting system conversion. As such, we are not providing assurances that procedures and internal controls were followed and adhered to in accordance with the federal, state, local policies and guidelines.

The Campus Accounting System Conversion Consulting Services engagement was approved by the Board of Trustees as part of the 2016-2017 Internal Audit Plan.

Background

The AS400 Campus Accounting module (AS400) was the accounting system used by school financial clerks to record school financial transactions related to campus activity funds for over 20 years. During school year 2015-2016, a decision was made by administration to replace the AS400 with School Funds Online (SFO) by Technology Resource Associates (TRA). School Funds Online is a web-delivered software application designed to automate the tracking of any funds collected and disbursed at the school level. School Funds Online (SFO) went live January 2017 and the AS400 ceased to be used for campus activity fund transactions in December 2016.

Internal Audit became aware of this conversion engagement after the software application (SFO) had been selected, but prior to the implementation stage. Consequently, Internal Audit offered to provide consulting services to Campus Accounting (an area within Financial Services), due to (i) inherent risks associated with conversion engagements, (ii) the potential to improve risk management, (iii) the potential of adding value, and (iv) improving efficiency within the District's operations.

Objective and Scope

The objective was to provide consulting services to Campus Accounting (CA) in the implementation of the new campus accounting system (SFO) based on discussions with management, best practices, and our knowledge and understanding of internal controls.

Our consulting engagement started in June 2016 and ended on February 2017. More specifically, it started after the software application (SFO) had been selected and ended when SFO went live.

Methodology

To achieve our objectives, we:

- Researched information security frameworks and best practices published by leading information security organizations.

- Attended meetings/conference calls with process owners and software vendor representatives. Topics such as internal controls, audit reports, application settings, future enhancements, user access administration, connectivity, and audit logs were discussed.

- Reviewed documentation/information related to (i) procurement process, (ii) data center, (iii) information security, (iv) data privacy, (v) internal controls, (vi) change management process, (vii) and application support provided by software vendor.

- Compared 100% of the amounts entered and verified accounts for completeness and accuracy from the ending balances in AS400 (December 2016) to beginning balances in SFO (January 2017).

Recommendations

		Category
1.	Any and all campus accounting procedures affected by SFO should be updated accordingly in the Campus Accounting Manual (CAM). ***Management's response/action:*** **Concur.** Campus Accounting staff has started to update the Campus Accounting Manual.	Policies and Procedures

2.	Until SFO security roles can be customized for Campus Accounting (CA) staff (who currently have system administrator roles), we recommend the following mitigating controls for:
	2.1. If not currently available, design and create a report and/or log that can show any and all system administrator activity by:
	    ▪ User,
	    ▪ Action taken,
	    ▪ Record or data modified,
	    ▪ Date, and
	    ▪ Timestamp
	
	2.2. Report and/or log mentioned above should be reviewed on a periodic basis to determine if unauthorized use by system administrators has occurred and/or attempted. This review should be carried out by someone independent of CA and with the appropriate level of skill and experience. Unauthorized activity should include a written explanation of any and all actions taken (including disciplinary if necessary) and filed with the District's Information Security Officer (ISO). Improprieties should be promptly communicated to the Chief Internal Auditor.
	
	2.3. Campus Accounting staff should not modify or request SFO to modify any future security settings within SFO without first collaborating with the District's ISO. If changes are made, they should be documented and filed with the District's ISO.
	
	Management's response/action: **Concur.** Recommendation will be implemented.
		Segregation of Duties

Recommendations	Category
3. Within any module in SFO, the social security number should be encrypted and masked upon screen display or printed for non-system administrators. ***Management's response/action:*** **Concur.** Although Campus Accounting staff previously updated system settings to encrypt and mask social security numbers, they will also ensure social security numbers still available for screen display are properly handled and secured.	Privacy
4. The District should include the following contractual terms in the vendor agreement with TRA: 4.1. Ensure TRA abides by the District's information security policies. 4.2. Ensure a software survivorship plan is in place in case TRA goes out of business so the District can continue using the software. 4.3. Ensure TRA reports all incidents of security issues directly to CA and the District's ISO in a timely and secure manner. 4.4. Ensure TRA has a robust data center which minimizes downtime, recovers services to the schools within a reasonable time frame, and utilizes an escalation process to resolve and communicate potential problems. 4.5. Align TRA's customer support hours to the District's normal hours and days on duty in a cost-effective way. ***Management's response/action:*** **Implemented**.	Access & Security
5. Campus Accounting (CA) should consult with the District's Information Security Officer (ISO) in all areas of user access management (i.e., user rights/roles, provisioning, user access reviews, and deprovisioning). The SFO user access review should be performed (and documented) at least annually by someone independent of CA and with the appropriate level of skill and experience. Recommendations made by the ISO and implemented by CA should be included in the CAM. ***Management's response/action:*** **Concur.** Recommendation will be implemented.	Access & Security
6. Approved users should be granted access to SFO by the District's ISO or designee after they have received adequate training on the use of the system as it relates to their role. The department providing the training should keep all training acknowledgements in accordance with the District's records retention schedule. ***Management's response/action:*** **Concur.** Current SFO granting access process will be formalized.	Access & Security
7. Consult with the District's ISO to create and develop a user agreement form on the proper use of the SFO system which is signed by all users (including system administrators) prior to receiving access. ***Management's response/action:*** **Concur.** Recommendation will be implemented.	Access & Security
8. Limit accessibility to SFO from approved District IP addresses. By doing this, the District can reduce the risk of (i) unauthorized access from non-District sites and (ii) wage and hour issues involving hourly employees working from home. ***Management's response/action:*** **Implemented.**	Access & Security (Includes Wage and Hour)

Recommendations	Category
9. Campus Accounting should consult with Accounts Payable and/or Procurement departments and establish a process to properly vet and document IRS defined 1099 vendors (e.g., one time vendors or vendors to be paid from club funds) added by CA staff within SFO. Once this class of vendors are properly vetted, at a minimum, the employee overseeing the CA staff should review and approve them before they are added to SFO. The entire process should be explained and included in the CAM. ***Management's response/action:*** **Concur.** Current vetting process will be formalized.	Vendor Management
10. Campus Accounting should create a comprehensive SFO training program that is available online using any of the platforms available to the District. ***Management's response/action:*** **Concur.** Recommendation will be implemented.	Training
11. Leverage SFO's document attachment upload feature wherever is available. By doing this, the District can take advantage of cost efficiencies related to digital paper management such as (not all inclusive): cost, storage, copying, printing, mailing, disposal, and recycling. In addition, the District can improve school/department support, document security and strengthen disaster recovery efforts. ***Management's response/action:*** **Concur.** Recommendation will be implemented.	Maximize Functionality