Columbus City Schools
Office of Internal Audit

General Ledger and Financial Reporting

Audit Report

Report Date: September 1, 2022

Table of Contents

Executive Summary

The Columbus City Schools (District) Office of Internal Audit (OIA) recently completed an audit of the General Ledger and financial reporting activities. These activities are primarily managed by the District's Controller within the Office of the Treasurer (Treasurer). This general audit evaluated objectives selected by OIA to assess the internal controls surrounding General Ledger and financial reporting processes. These internal controls were put in place by the Treasurer as well as service providers with which the District contracts for financial services that facilitate financial transactions with vendors and customers.

OIA initiated this audit after the Controller unexpectedly left employment with the District in March 2021 and it became clear to the OIA staff that the tasks he performed were not fully documented. Auditors determined that this lack of documentation increased the risk that financial transactions may not be complete and accurate. Therefore, our audit objectives were designed to ensure that management took steps to minimize this risk and ensure that tasks related to the General Ledger and financial reporting processes were appropriately completed by Treasurer staff.

During closure of the District's financial transactions in preparation for the June 30, 2021, year-end financial statements, the Treasurer consulted with Akron Public Schools for best practice guidance. The duties previously performed by the Controller have been assigned to various Executive Directors within the Treasurer's Office. that affect the General Ledger.

Our audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* established by the Institute of Internal Auditors. Our audit included such procedures as we deemed necessary to provide reasonable assurance regarding the audit objectives. Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. The internal audit function helps an organization accomplish its objectives through a systematic, disciplined approach to evaluating and improving the effectiveness of risk management, control, and governance processes.

OIA reported two issues and developed five associated recommendations. OIA rated the risk associated with the two issues as follows:

High	Moderate	Low
0	2	0

During the course of the audit, we made Treasurer's management aware of our issues and recommendations for improvement. Good discussion took place regarding the recommendations. OIA appreciates the cooperation extended to us and the assistance of all staff we interacted with as we performed our audit.

The OIA issues noted during the audit are classified as follows:

Risk Ratings, defined:

1 – High/unacceptable risk requiring immediate corrective action;

2 – Moderate/undesirable risk requiring future corrective action; and

3 – Low/minor risk that management should assess for potential corrective action**.**

Issues	Risk Rating		
	1	2	3
Objective 1: **To determine whether written business objectives exist for the Controller's functions and whether department sections have business objectives that align with those of the Treasurer. Additionally, we sought to determine whether metrics were tracked for the functions that were reporting to the Controller and whether they were routinely compared to established benchmarks.**			
Issue 1 - Treasurer's management has not fully implemented business objectives or metrics for its functions as they relate to the duties that were previously performed by the Controller and are now assigned to Executive Directors of the Treasurer's office that affect the General Ledger.		X	
Objective 2: To determine whether appropriate governance exists over the Controller's roles and responsibilities and the tested control processes: **a. Period, year-end reporting procedures; and** **b. Controller activities related to third-party service organizations' System and Organization Controls/Statement on Standards for Attestation Engagements (SOC/SSAE) reporting.**			
Issue 2 - Treasurer's management has not consistently requested, obtained, and reviewed third-party service organization SOC/SSAE reports. Additionally, management has not implemented suggested user consideration controls or monitoring activities included in one SOC report.		X	

Background

When the Controller unexpectedly left the District in March 2021, the Treasurer's office underwent a reorganization to reassign the Controller's duties. The Controller directed the day-to-day operations of the Treasurer's office, instructed department managers,

including in Payroll and Accounts Payable, and managed grant financial reporting. Additionally, the Controller was responsible for performing the monthly and annual financial closing procedures and cash management procedures.

To assess the General Ledger and financial reporting internal controls, our audit objectives focused on the management, processing, and functions as defined by the job duties listed in the job description for the Controller position and other responsibilities as assigned by the Treasurer.

Results of the General Ledger Audit - Issues and Recommendations:

Issue 1 – Treasurer's management has not fully implemented business objectives or metrics for its functions as they relate to the duties that were previously performed by the Controller and are now assigned to Executive Directors of the Treasurer's office that affect the General Ledger. (Risk Rating: Moderate)

In FY18, the Treasurer's office contracted with accounting firm Rea & Associates to conduct a variety of consulting services, primarily focused on process evaluation and improvement. Rea & Associates issued the resulting Opportunity Study in FY20, which contained many recommendations that would improve processes and efficiencies. This work did not include a review of the duties performed by the Controller.

The Rea & Associates report, dated March 2020, was delivered with accompanying process manuals for the following departments and functions: Fixed Assets, Accounts Payable, Payroll, Payroll Supervisor, and Disbursements. Each manual contained specific performance metrics, but none were developed for the Controller position.

The Treasurer has begun to develop spreadsheet and the data sources for the payable performance metrics comparison to its benchmarks, but has not begun the same for the remaining department benchmarks.

Performance metrics enable the Treasurer to monitor and measure actual department performance against pre-established benchmarks to identify performance gaps and deficiencies. Identifying opportunities for improvement can then prompt mitigation measures that, when implemented, will help departments to meet established goals and objectives.

In the absence of monitoring departmental performance, management cannot identify opportunities for improvement or timely implement mitigation measures to ensure that departments continue to operate at the highest level. Such monitoring should include the period and year-end closing duties previously assigned to the Controller but reassigned to the Executive Directors in the Treasurer's office.

Recommendations

1. For the previous Controller job duties and functions that were assigned to others, the Treasurer should develop business objectives, performance metrics, and benchmarks at the Executive Director level.

2. The Treasurer should implement procedures to routinely gather and analyze departmental performance metrics for departments with activities that affect the General Ledger. These metrics should periodically be reviewed for accuracy and compared to established benchmarks.

3. The Treasurer should develop and implement mitigation strategies where performance as indicated by established metrics are found to vary from the established benchmarks for optimal performance.

Management Response: The Treasurer's Office has and will continue to evaluate department metrics and consider courses of action for implementation as said metrics are identified.

Implementation Date: Ongoing

Process Owner: Stan Bahorek, Treasurer/CFO

Issue 2 – Treasurer's management has not consistently requested, obtained, and reviewed third-party service organization SOC/SSAE reports. Additionally, management has not implemented suggested user consideration controls or monitoring activities included in one SOC report. (Risk Rating: Moderate)

The District uses several service organizations to process financial transactions, such as making electronic payments to vendors and to collecting revenue. These service organizations have their own system of controls and internal control environments. They have an annual review of their control processes conducted by an independent auditor who issues a System and Organization Control (SOC) report. These reviews are conducted following standards promulgated by the American Institute of Certified Public Accountants (AICPA) and culminate in one of the following three types of reports:

- **SOC 1:** This engagement reports on whether a service organization has effective internal controls in place pertaining to financial reporting in order to protect client data.
- **SOC 2:** This audit assesses internal controls related to information security, including data availability, confidentiality, privacy, and processing integrity.
- **SOC 3:** Similar to a SOC 2 report, this report attests to the suitability of internal security controls without providing any specific descriptions of the organization's systems. Whereas SOC 1 and SOC 2 reports are available to customers who use the provider's services, a SOC 3 report is intended for the general public, allowing potential customers to see that the organization is compliant without revealing any mission-critical or proprietary information about their operations and systems.

SOC reports, regardless of the type, are further differentiated as Type 1 or Type 2. A Type 1 SOC report demonstrates that an organization has the appropriate controls in place for managing risk as of the date the report is issued. A Type 2 SOC report, on the other hand, focuses on how effective those controls are in practice.

The Treasurer's has outsourced the following financial functions to the below mentioned service organizations:

Payrix (Infinite Campus) and Local Level

Card processing/gateway
Colocation services

Avid Xchange

Scanning services
Indexing services
Payment Conversion services
On-boarding services
Support services

Treasurer's management was able to obtain and provide a SOC 1, Type 2, report for Avid Xchange, the third-party service provider responsible for making payments to vendors on the District's behalf. There is no requirement establishing that these SOC reports must be submitted to the District within a certain amount of time once completed and received by the vendor. The report detailed the effectiveness of their internal controls pertaining to financial reporting and the security of client data. The report identified deficiencies and gaps with implications for the internal controls that should be in place for a user, such as the District. Specifically, the auditors that generated the SOC report provided specific guidance for user organizations on how they should be implementing compensating control procedures that can mitigate known service providers' deficiencies and gaps to enhance the effectiveness of the service provider control processes.

Treasurer's management was able to provide an attestation for compliance onsite assessment for service providers, dated June 2018, for Payrix (Infinite Campus) and Local Level. Both of these vendors collect revenue on behalf of the District. These compliance reports were submitted by Payment Card Industry (PCI) Data Security Standards (DSS). These reports were not created adhering to AICAP standards and were not an annual review of the organization's control processes conducted by an independent auditor who issues a SOC report.

The PCI Report on compliance is used to verify that a merchant is compliant with PCI DSS. The policies and procedures included in PCI DSS were developed to enhance the security of card-based transactions and protect cardholder data against fraud and other misuses of their personal information.

Treasurer's management did submit compensating controls, which they felt could meet the user considerations identified in the SOC report obtained relating to AvidXchange. Yet, OIA was unable to test those controls as management could not provide information or data to support the user controls' operations and their effectiveness. This could enable errors to occur, which could prevent the Department from meeting its objectives.

By not obtaining and reviewing SOC reports in a timely manner, key functions of the Treasurer could be impacted by third-party vendors who do not have effective internal control environments. These possible failures increase the risk of negatively affecting operations and could reflect unfavorably upon the District.

Recommendations

4. Treasurer's management should review SOC/SSAE reports upon receipt and promptly take necessary action. This action could involve contacting the third-party service provider to resolve any issues on their end or to implement suggested user control considerations included in the report. For any compensating controls, supporting documentation should be maintained to evidence the control operations and their effectiveness. Periodic reviews should occur by Treasurer's management to ensure the controls are operating as management intended with competent evidence of the review and acceptance.

5. Treasurer's management should consider including a requirement in all relevant third-party service provider contracts that SOC reports are to be submitted to the District within 30 days of issuance to their organization. This will help to minimize the time of exposure when processes are identified to not meet standards.

Management Response:

The Treasurer's Office agrees that third-party risk management is of great importance. Regarding those functions for which the Treasurer's Office has direct oversight, the Office will work to identify third-party vendors and relevant reports (SOC, PCI-DSS, etc.) and a process to request and review those reports on an annual basis.

Implementation Date: 12/31/2022

Process Owner: Stan Bahorek, Treasurer/CFO

Audit Objectives

OIA established the following objectives for the audit:

- To determine whether written business objectives exist for the Controller's functions and whether department sections have business objectives that align with those of the Treasurer. Additionally, we sought to determine whether metrics were tracked for the functions that were reporting to the Controller and whether they were routinely compared to established benchmarks.

- To determine whether appropriate governance exists over the Controller' roles and responsibilities and the tested control processes:

  Period, year-end closing procedures:

  - Period, year-end reporting procedures;
  - Closing journal entries (manual);
  - Period 13 accounting procedures;
  - Automated closing procedures;
  - Authorization/approval process; and
  - Closing procedures to identify significant reporting variances, fraud, and remedy procedures.

  Controller activities related to third-party service organizations' SOC/SSAE reporting:

  - Obtain the third-party administrator's SOC/SSAE Reports (Avid, Procurement Card, Lockbox, and Cash Collection Points).
  - Evaluate control procedures in place that mitigate TPA's, service provider, deficiency/gaps identified.
  - Review and evaluate the control(s) in place to mitigate TPA's reported deficiencies and gaps.

Audit Scope

The period from which transactions and other periodic activities were selected for examination were generally July 1 through July 31, 2021. However, OIA will select transactions and/or evidence of activities from other periods should audit results dictate such selection.

.

Methodologies

To accomplish the audit objectives, OIA generally used inquiry, observation, and document/record examination and the following tasks as they relate to those objectives:

- Reviewed various relevant authoritative literature;
- Reviewed relevant District Board of Education (BOE) policies and administrative guidelines;
- Reviewed the Controller job specifications and duties;
- Reviewed best practices in month-end and periodic closing procedures and processes;
- Reviewed relevant Auditor of State polices and compliance requirements, guidance, and best practices;

- Reviewed contractor-produced reports for the Treasurer Office Lean Six Sigma Project Opportunity Study (Rea & Associates) and Risk Assessment (Clark Schaefer Consulting);
- Reviewed prior relevant OIA audits;
- Interviewed selected Treasurer's Office management and staff;
- Reviewed System and Organization Controls (SOC) reports for third-party service organizations providing financial services to the District; and
- Reviewed and considered the Committee on Sponsoring Organizations of the Treadway Commission (COSO) Integrated Framework Principles.