Assessment and Evaluation of Oracle's IT General Controls and Application Controls
School District of Philadelphia
Fiscal Year 2021

City Controller
Rebecca Rhynhart

June 2022

CITY OF PHILADELPHIA

OFFICE OF THE CONTROLLER
1230 Municipal Services Building
1401 John F. Kennedy Boulevard
Philadelphia, PA 19102-1679
(215) 686-6680   FAX (215) 686-3832

REBECCA RHYNHART
City Controller

CHRISTY BRADY
Deputy City Controller

Joyce Wilkerson, President
Philadelphia Board of Education
440 N. Broad Street
Suite 101
Philadelphia, PA 19130

Tuesday, June 14, 2022

Dear Mrs. Wilkerson,

As part of our audit of the Philadelphia School District's Annual Comprehensive Financial Report (ACFR) for the fiscal year ended June 30, 2021, the Office of the City Controller retained Eisner Advisory Group, LLC (EisnerAmper) to perform an assessment of Information Technology (IT) general controls and application controls related to the District's new Oracle system. Attached is EisnerAmper's report, which identified one significant deficiency and two control deficiencies. Please note, information from this report is also included in our annual report on internal control and on compliance and other matters for fiscal year 2021.

The District provided a thorough response to the findings in our report, including steps to remedy the findings. We encourage the District to remediate the findings to ensure that the new Oracle system operates with appropriate safeguards in place. We thank the District for its thoughtful response and plan of action.

Respectfully submitted,

Rebecca Rhynhart
City Controller

CC: Board of Education members
       Dr. William Hite, Superintendent
       Uri Monson, Chief Financial Officer, Philadelphia School District
       Marcy Blender, Deputy Chief Financial Officer and Comptroller

SCHOOL DISTRICT OF PHILADELPHIA
REPORT ON INTERNAL CONTROL AND ON
COMPLIANCE AND OTHER MATTERS
EXECUTIVE SUMMARY

Why the Controller's Office Conducted the Audit

In accordance with the Philadelphia Home Rule Charter, the Office of the City Controller engaged Eisner Advisory Group, LLC (EisnerAmper) to perform an assessment of the Information Technology (IT) general controls and applications related to the Philadelphia School District's (District) new Oracle system. The Oracle system is a multi-year modernization initiative by the School District to replace its legacy Finance system. It will also replace the District's legacy Human Resources Information System, which is currently in the process of being implemented. The assessment was to evaluate whether the IT general controls and application controls were efficiently designed, implemented, and operating as part of the Office of the City Controller's audit of the School District's Annual Comprehensive Financial Report (ACFR) for the fiscal year ended June 30, 2021.

Report Findings

Based on its potential impact to the District's ACFR, the assessment identified one significant deficiency and three control deficiencies that require management's attention. The findings are as follows:

Significant Deficiency
A formally documented Segregation of Duties (SoD) policy, including identification of incompatible roles, responsibilities, and permissions was not established. Periodic reviews of user access have not been performed since the Oracle system went live on July 1, 2020. Additionally, a documented security program or policy, which should include the District's responsibilities over the Oracle system, was not provided. As a result, there may be users with access not commensurate with their job responsibilities and users may have access across incompatible roles, responsibilities, and permissions within the system, potentially allowing users to bypass system controls.

Control Deficiencies
Of 25 terminated employees tested, one user's system access was not disabled in a timely manner. If unauthorized system access is maintained, a user could potentially perform unauthorized transactions.

There was no formal, documented review of the Oracle Fusion Service Organization Control (SOC) 1 report. SOC reports are AICPA defined reports which are performed by Public Accounting firms to evaluate and report on the controls at a third-party service provider. SOC reports allow management and auditors to gain comfort over controls at a third-party service provider without the need to perform their own audit procedures.

A formal policy for configuration changes, including the procedures for requesting changes from Oracle and the supporting vendor, nor a formal list of change requests, including Oracle requested changes, configuration changes, and emergency changes, was maintained. Without documented configuration change management process, there is a risk of unauthorized changes, and changes that have not been tested before implementation, which could affect the system's operation.

Why the Controller's Office Conducted the Audit

The Controller's Office has presented a number of recommendations to address the findings in this report. The recommendations include formally documenting a SoD policy and configuration change policy, as well as removing terminated employee access in a timely manner and formally reviewing SOC 1 reports.

Assessment and Evaluation of Oracle's IT General Controls and Application Controls

Hon. Rebecca Rhynhart
City Controller
City of Philadelphia
1401 JFK Boulevard, 12th Floor
Philadelphia, Pennsylvania 19102

We have concluded our engagement to perform an evaluation of the general and application controls of information technology functions of the School District of Philadelphia's Oracle Enterprise Resource Planning System (the Oracle system). This engagement was agreed to by the City of Philadelphia – Office of the Controller (the Controller's Office) and was performed solely to assist in evaluating the IT general controls and application controls for the Oracle system in connection with the Controller's Office audit of the School District of Philadelphia's (the school district's) fiscal year 2021 Annual Comprehensive Financial Report (ACFR).

Management of the School District is responsible for the operations of, and internal controls, over the Oracle system. The sufficiency of the scope and procedures of our engagement is solely the responsibility of the management of the Controller's Office. Consequently, we make no representations regarding the sufficiency of the scope and procedures described in the attached document either for the purpose for which this report has been requested or for any other purpose.

The Engagement was performed in accordance with applicable professional standards, including the Statements on Standards for Consulting Services issued by the American Institute of Certified Public Accountants (AICPA). EisnerAmper did not perform an audit, review, or compilation in accordance with Generally Accepted Government Auditing Standards or with attest standards established by the AICPA.

The procedures performed were limited to those described herein based on the documents provided, interviews and process walkthroughs with the city and School District of Philadelphia staff, and other information obtained including whether internal controls were placed in operation and adequately designed as of the June 30, 2021. Information obtained subsequent to the date of this report may affect this analysis. The procedures were performed solely with respect to the above referenced engagement. This report is not to be reproduced, distributed, disclosed or used for any other purpose.

We have attached observations and recommendations regarding IT general controls and application controls resulting from the consulting engagement for the consideration of the Controller's Office. We assessed application controls, and IT general controls over security management, access controls, segregation of duties, configuration management, and contingency planning. The results of our procedures for the IT general controls identified a potential Significant Deficiency.

The procedures performed and related observations and recommendations are described in the attached document. We performed our procedures during the months of November 2021 through February 2022.

EISNERAMPER

Philadelphia, Pennsylvania
May 23, 2022

City of Philadelphia – Office of the Controller
Assessment and Evaluation of the School District of Philadelphia's Oracle System
IT General Controls and Application Controls
As of June 30, 2021

Table of Contents

City of Philadelphia – Office of the Controller
Assessment and Evaluation of the School District of Philadelphia's Oracle System
IT General Controls and Application Controls
As of June 30, 2021

Executive Summary

The Controller's Office engaged Eisner Advisory Group, LLC (EisnerAmper), to perform an assessment of Information Technology (IT) general controls and application controls related to the School District of Philadelphia's Oracle system.

We conducted this engagement in accordance with Statements on Standards for Consulting Services issued by the AICPA. The scope of the assessment was limited to internal controls in place and designed as of June 30, 2021. Our review procedures were performed during the months of November 2021 through February 2022, related to testing of the design, implementation, and operating effectiveness of the IT general controls and application controls.

A summary of observations and potential impact are noted below.

Summary of Objective, Scope and Methodology

The objective of the EisnerAmper consulting engagement was to evaluate the IT general controls and application controls designed, implemented, and operating effectively for the School District of Philadelphia's Oracle system in support of the Controller's Office audit of the School District of Philadelphia's Annual Comprehensive Financial Report (ACFR). The scope of the assessment included the internal controls in place as of June 30, 2021.

Our assessment over the application controls, as requested by the Controller's Office, was focused on the completeness, accuracy, and validity of processing data, as well as the confidentiality and availability of data as it applies to the following Oracle functions: Accounts Payable, Accounts Receivable, Cash Management and General Ledger.

In addition, our engagement was structured to address the following five (5) areas for the IT general controls as requested by the Controller's Office:

1. *Security Management* - the controls designed and placed into operation to provide reasonable assurance that security management is effective.

2. *Access Controls* - the controls designed and placed into operation to provide reasonable assurance that access to computer resources (data, equipment, and facilities) is reasonable and restricted to authorized individuals.

3. *Configuration Management* - the controls designed and placed into operation to provide reasonable assurance that changes to information system resources are authorized and systems are configured and operated securely and as intended.

4. *Segregation of Duties* - the controls designed and placed into operation to provide reasonable assurance that incompatible duties are effectively segregated.

5. *Contingency Planning* - the controls designed and placed into operation to provide reasonable assurance that contingency planning (1) protects information resources and minimizes the risk of unplanned interruptions and (2) provides for recovery of critical operations should interruptions occur.

City of Philadelphia – Office of the Controller
Assessment and Evaluation of the School District of Philadelphia's Oracle System
IT General Controls and Application Controls
As of June 30, 2021

Summary of Observations

Below is a summary of key observations noted through the procedures performed for this engagement. Based upon its potential impact on the School District of Philadelphia's ACFR, each key finding listed below was assigned a rating.[1] Additional details for these key observations are provided in the detailed section of our report.

Area	Findings	Potential Impact
Application Controls	No exceptions noted.	Not applicable
Security Management	There is no formal review of the Oracle Fusion SOC 1 report.	Control Deficiency
Access Controls and Segregation of Duties	Incompatible roles, responsibilities, and permissions are not formally and comprehensively identified. Periodic user access reviews have not been performed.	Significant Deficiency
	One out of 25 terminated users tested did not have their system access disabled in a timely manner.	Control Deficiency
Configuration Management	A formal configuration change management policy is not maintained. A formal list of changes is not maintained.	Control Deficiency
Contingency Planning	No exceptions noted.	Not applicable

---

[1] The AICPA's *Professional Standards (Clarified)* AU-C Section 265.07 states that a deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. AU-C Section 265.07 provides the following definitions:

Material Weakness – This is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis.

Significant Deficiency – This is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness yet important enough to merit attention by those charged with governance.

City of Philadelphia – Office of the Controller
Assessment and Evaluation of the School District of Philadelphia's Oracle System
IT General Controls and Application Controls
As of June 30, 2021

Detailed Scoping Areas

For the application controls, we focused on several control elements as follows:

Completeness Checks	Controls ensure records processing from initiation to completion.
Validity Checks	Controls ensure only valid date is input or processed.
Identification	Controls ensure unique, irrefutable identification of all users.
Authentication	Controls provide an application system authentication mechanism.
Authorization	Controls ensure access to the application system by approved business users only.
Input Controls	Controls ensure data integrity feeds into the application system from upstream sources.
Forensic Controls	Controls ensure scientifically and mathematically correct data, based on inputs and outputs.

City of Philadelphia – Office of the Controller
Assessment and Evaluation of the School District of Philadelphia's Oracle System
IT General Controls and Application Controls
As of June 30, 2021

Our engagement was structured to address the five (5) areas for IT general controls. Within each area, we focused on several control elements as follows:

Security Management	- A Security management program is in place - Periodic assessments and validation of risk - Security control policies and procedures - Security awareness training and other security related personnel issues - Periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices - Remediation of information security weaknesses - Security over activities performed by external third parties
Access Controls	- Protection of information system boundaries - Identification and authentication mechanisms - Authorization controls - Protection of sensitive system resources - Audit and monitoring capability, including incident handling - Physical security controls
Configuration Management	- Configuration management policies, plans, and procedures - Current configuration identification information - Proper authorization, testing, approval, and tracking of all configuration changes - Routine monitoring of the configuration - Updating software on a timely basis to protect against known vulnerabilities - Documentation and approval of emergency changes to the configuration
Segregation of Duties	- Segregation of incompatible duties and responsibilities and related policies - Control of personnel activities through formal operating procedures, supervision, and review
Contingency Planning	- Protection of information resources and minimizing the risk of unplanned interruptions - Provision for recovery of critical operations should interruptions occur, including effective: - Assessment of the criticality and sensitivity of computerized operations and identification of supporting resources; - Steps taken to prevent and minimize potential damage and interruption; - Comprehensive contingency plan; and - Periodic testing of the contingency plan, with appropriate adjustments to the plan based on testing.

City of Philadelphia – Office of the Controller
Assessment and Evaluation of the School District of Philadelphia's Oracle System
IT General Controls and Application Controls
As of June 30, 2021

Background Information on the Oracle ERP System
The Oracle system is a modernization initiative created by the School District of Philadelphia. The system replaced the legacy Finance system. It is also planned to replace the legacy Human Resources Information System (HRIS), which is currently in process of being implemented.

Timeline and Implementation
The Oracle project has been a multiyear effort which began in 2018. In July 2020, the Finance modules went live. A specific timeline for the HRIS modules has not been communicated.

System Architecture
The core platform for the Oracle system is Oracle Fusion. The application is hosted on within the Oracle cloud. Oracle system is a solution configured to meet the requirements of the School District.

Detailed Results

Observations

Below is our summary and the supporting detail for the key observations noted through the procedures performed for this engagement. Our observations include the detail of the condition, the criteria, the potential cause, the effect, and our recommendation.

Access Controls and Segregation of Duties

1. <u>Review and Approval of Access, including Segregation of Duties</u>
   Potential Impact: **Significant Deficiency**

   Condition: A formally documented Segregation of Duties (SoD) policy, including identification of incompatible roles, responsibilities, and permissions, has not been established. Users have been assigned access based upon job function role and location, however the specific access permissions of the roles have not been reviewed by the School District of Philadelphia. Due to this, identification of incompatible permissions within roles or across roles has not been performed. In addition, a periodic user access review has not been performed since the implementation of the system which went live July 1, 2020. Finally, a documented security program or policy, which includes the School District of Philadelphia's responsibilities over the Oracle system, was not provided.

   Criteria: Although the Oracle system is a vendor hosted system, there are aspects of the security and provisioning of access to the system, which is the responsibility of the School District of Philadelphia. Incompatible roles, responsibilities, and permissions should be established to enforce SoD in both the provisioning and the periodic reviewing of user access.

   Potential Cause: As part of the implementation of the system, there was not a required step to identify incompatible user access permissions. A periodic review of access has not been performed due to the current focus on the implementation of the Oracle HR system.

   Effect: There may be users with access not commensurate with their job responsibilities. In addition, users may have access across incompatible roles, responsibilities and permissions within the system, thereby potentially allowing a user to bypass system controls.

   Recommendation: The School District of Philadelphia should formally identify the areas of responsibility related to security and provisioning of access related to the Oracle system and include them in an overall security program or policy. As part of this security program or policy, a requirement for the performance of a periodic access review should be included. There should also be a comprehensive document that clearly identifies incompatible roles, responsibilities, and permissions. These SoD considerations should be included in the periodic access reviews.

2. Deprovisioning of Access

    Potential Impact: **Deficiency**

    Condition: For one (1) out of 25 terminated users tested, the user's system access was not disabled in a timely manner. The user was suspended without pay, awaiting a board decision for termination, however the user's access was not disabled during the period between suspension and approval of termination.

    Criteria: When a user is suspended or terminated, their system access should be disabled in a timely manner.

    Potential Cause: Human Resources received notification from the Labor Relations team after the board approved the termination. At which time, the user's access was disabled. The date of suspension awaiting approval of termination was not provided to trigger the disabling of access.

    Effect: Unauthorized system access is maintained, allowing a user to perform unauthorized transactions.

    Recommendation: When a user is suspended awaiting termination, notification should be provided to Human Resources who can update the system in a timely manner to trigger the user's access to be disabled.

Security Management

3. Monitoring of Third Parties
   Potential Impact: **Deficiency**

   Condition: There is no formal, documented review of the Oracle Fusion Service Organization Control (SOC) 1 report.

   Criteria: Reliance on a third party to support key processes require formalized monitoring controls by the School District of Philadelphia to ensure that any issues at the third party are evaluated for impact to the School District of Philadelphia. In addition, hand-off controls between the third party and the School District of Philadelphia should be identified and formalized. SOC reports are AICPA defined reports which are performed by Public Accounting firms to evaluate and report on the controls at a third-party service provider. SOC reports allow management and auditors to gain comfort over controls at a third party service provider without the need to perform their own audit procedures.

   Potential Cause: The Oracle Fusion SOC 1 report was not originally made available by the vendor.

   Effect: Formal review of SOC reports is not documented. In addition, there is an increased risk of unauthorized access.

   Recommendation: An annual review of the Oracle Fusion, and other applicable SOC reports should be formally documented. This includes evaluating any exceptions in the report, mapping of Complementary User Entity Controls (CUECs) to controls within the School District of Philadelphia, and review of any subservice organization's SOC report.

Configuration Management

4. <u>Formal Policy for Configuration Changes</u>
   Potential Impact: **Deficiency**

   Condition: A formal policy for configuration changes, including the procedures for requesting changes from Oracle and the supporting vendor, is not maintained. In addition, a formal list of change requests, including Oracle requested changes, configuration changes, and emergency changes, is not maintained.

   Criteria: A formal configuration change management policy should be maintained that captures the various types of changes that can be made to the system and required steps in the identification, testing, approval, and implementation of changes. As defined by the policy, a formal list of change requests should be maintained.

   Potential Cause: During the Oracle system implementation, the supporting vendor was responsible for defining and enforcing the change management process. When the system was implemented, the School District of Philadelphia established a change management process, however it was not formally documented.

   Effect: Without documented configuration change management process, there is a risk of unauthorized changes, and changes that have not been tested before implementation. This could affect the operations of the system.

   Recommendation: A formal policy for configuration changes should be maintained that captures the various types of changes that can be made to the system. The policy should include the required steps in the identification, testing, approval, and implementation of changes. As defined by the policy, a formal list of change requests should be maintained, such as with a ticketing system, or be maintained by those who are not responsible for initiating, performing, testing or approving changes.

Management's Response

RESPONSE to 2021-001 INADEQUATE REVIEW OF ACCESS CONTROLS AND SEGREGATION OF DUTIES

A new state of the art cloud-based Oracle Enterprise Resource Planning Finance System ("ERP Finance System") went live starting with the fiscal year beginning July 1, 2020. This was a major accomplishment for the School District of Philadelphia ("The District") because it allowed remote access to the ERP System during the Covid-19 Pandemic and significantly improved financial controls and transparency of financial information.

The District appreciates the initial assessment and evaluation of the ERP Systems' IT General and Application Controls which was performed by Eisner Advisory Group, LLC on behalf of the Office of the City of Philadelphia Controller for Fiscal Year 2021 (the first year in production for a three-year implementation). The District acknowledges that we will take corrective actions for the one significant deficiency related to access controls and segregation of duties and are pleased that all other observations in the remaining five key areas reviewed were either not applicable because there were no exceptions noted or a control deficiency of a non-major or non-significant consequence to compromise the systems' financial controls and data integrity. We commit all such findings will be rectified timely.

The District agrees with the recommendations for Finding 2021-001 and will implement the following initiatives within the next six months and continue to keep them updated periodically:

- Formally document the areas of responsibility related to access to the ERP Finance System.
- Expand upon the current security program/policy to include a more comprehensive policy with detailed procedures and documentation.
- Based upon this documentation and policy, annually perform a system access review which will be a requirement included in the policy. Segregation of duty analyses will be included as part of this review.
- Prepare a comprehensive formal document which will clearly identify incompatible roles, responsibilities and security permissions.

The District takes very seriously the security and controls associated with our ERP Finance System. During the implementation of the Oracle ERP Finance system, measures were taken to review all roles that would be assigned to System Users so that they could perform their necessary job functions. Although the roles and privileges were not formally documented, roles and privileges were reviewed by the Information Technology Office and System Module Team Leads, and assigned based upon segregation of duties and internal control and regulatory compliance considerations.

A documented security program/policy was created as part of the ERP System implementation and provided to the auditors. However, SDP commits that the policy will be updated to include a more comprehensive and detailed list of roles and privileges. Any roles that are added subsequently will be updated within the policy document, along with implementing a periodic annual review of all users and roles assigned to them.

The District thanks our auditors for recognizing the achievement and accomplishment of implementing our new ERP Finance System. We also appreciate that during the Exit Conference they recognized the relatively few general and application control findings associated with the implementation of a new ERP System. This was accomplished remotely during a World-wide pandemic.