STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2021-004
July 2020

PALM BEACH COUNTY DISTRICT SCHOOL BOARD

Oracle PeopleSoft Applications and Focus Student Information System

Sherrill F. Norman, CPA
Auditor General

Board Members and Superintendent

During the period March 2019 through December 2019, Donald E. Fennoy II, Ed.D. served as Superintendent of the Palm Beach County Schools and the following individuals served as School Board Members:

	District No.
Barbara McQuinn	1
Chuck E. Shaw, Vice Chair	2
Karen M. Brill	3
Erica Whitfield	4
Frank A. Barbieri Jr., Esq., Chair	5
Marcia Andrews	6
Dr. Debra Robinson	7

The team leader was Stephanie J. Hogg, CISA, and the audit was supervised by Heidi Burns, CPA, CISA.

Please address inquiries regarding this report to Heidi Burns, CPA, CISA, Audit Manager, by e-mail at heidiburns@aud.state.fl.us or by telephone at (850) 412-2926.

This report and other reports prepared by the Auditor General are available at:

FLAuditor.gov

Printed copies of our reports may be requested by contacting us at:

State of Florida Auditor General

Claude Pepper Building, Suite G74 · 111 West Madison Street · Tallahassee, FL 32399-1450 · (850) 412-2722

PALM BEACH COUNTY DISTRICT SCHOOL BOARD

Oracle PeopleSoft Applications and Focus Student Information System

SUMMARY

This operational audit of Palm Beach County District School Board (District) focused on evaluating selected information technology (IT) controls applicable to Oracle PeopleSoft Applications and Focus Student Information System and on the progress that the District had made, or was in the process of making, in addressing Finding 7 in our report No. 2019-218. Our audit disclosed the following:

Finding 1: Certain District IT security controls need improvement to ensure the confidentiality, integrity, and availability of District data and IT resources.

BACKGROUND

The Palm Beach County School District (District) is part of the State system of public education under the general direction of the Florida Department of Education. The governing body of the District is the Palm Beach County District School Board (Board), which is comprised of seven elected members. The appointed Superintendent of Schools is the Executive Officer of the Board. During the 2018-19 fiscal year, the District operated 184 schools and centers, sponsored 48 charter schools, and reported 232,534 unweighted full-time equivalent students.

The District uses Oracle PeopleSoft Applications (PeopleSoft Applications) to process and report finance and human resources transactions and the Focus Student Information System (Focus) for the recording, processing, and reporting of student record information. In addition, the District maintains and manages the network domain, application, Web, and database servers, and database management systems supporting Peoplesoft Applications and Focus.

FINDINGS AND RECOMMENDATIONS

Finding 1: Security Controls

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed that certain security controls need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising the confidentiality of District data and related IT resources. However, we have notified appropriate District management of the specific issues.

Without appropriate security controls, the risk is increased that the confidentiality, integrity, and availability of District data and related IT resources may be compromised.

Recommendation: We recommend that District management improve IT security controls to ensure the confidentiality, integrity, and availability of District data and IT resources.

PRIOR AUDIT FOLLOW-UP

The District had taken corrective actions for the applicable finding included in our report No. 2019-218.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this IT operational audit from September 2019 through December 2019 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the audit findings and our conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for the audit findings and our conclusions based on our audit objectives.

This IT operational audit focused on evaluating selected significant District IT controls applicable to the Oracle PeopleSoft Applications (PeopleSoft Applications) and Focus Student Information System (Focus) during the period March 2019 through December 2019, and selected actions subsequent thereto. For those areas addressed by this audit, our audit objectives were:

- To determine the effectiveness of selected IT controls in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources.
- To determine whether management had corrected, or was in the process of correcting, deficiencies disclosed in Finding 7 of our report No. 2019-218.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

In planning and conducting our audit, we identified internal controls significant to our audit objectives by considering the internal control integrated framework established by the Committee of Sponsoring Organizations (COSO)[1] and adapted for a government environment within the *Standards for Internal Control in the Federal Government* issued by the United States Government Accountability Office. That framework is illustrated in the following table.

[1] The Committee of Sponsoring Organizations (COSO) of the Treadway Commission was established in 1985 to develop guidance in the areas of risk and control which enable good organizational governance and reduction of fraud. Pursuant to their mission, COSO developed a framework for internal control that consists of five components and 17 underlying principles.

COSO Internal Control Integrated Framework

Internal Control Component	Description	Underlying Principles (To be Applied by the Board and District Management)
Control Environment	Standards, processes, and structures that provide the basis for carrying out internal control across the organization. Represents the foundation on which an effective internal control system is built.	• Demonstrate commitment to integrity and ethical values. • Exercise oversight responsibility. • Establish structures and reporting lines and assign authorities and responsibilities. • Demonstrate commitment to a competent workforce. • Hold individuals accountable for their responsibilities.
Risk Assessment	Management's process to consider the impact of possible changes in the internal and external environment and to consider actions to mitigate the impact. The basis for how risks will be managed.	• Establish clear objectives to define risk and risk tolerances. • Identify, analyze, and respond to risks. • Consider the potential for fraud. • Identify, analyze, and respond to significant changes that impact the internal control system.
Control Activities	Activities in the form of policies, procedures, and standards that help management mitigate risks. Control activities may be preventive in nature or detective in nature and may be performed at all levels of the organization.	• Design control activities to achieve objectives and respond to risks. • Design control activities over technology. • Implement control activities through policies and procedures.
Information and Communication	Information obtained or generated by management to support the internal control system. Communication is the dissemination of important information to help the organization meet requirements and expectations.	• Use relevant and quality information. • Communicate necessary information internally to achieve entity objectives. • Communicate necessary information externally to achieve entity objectives.
Monitoring	Periodic or ongoing evaluations to verify that the internal control system is present and functioning properly.	• Conduct periodic or ongoing evaluations of the internal control system. • Remediate identified internal control deficiencies on a timely basis.

We determined that the internal control components significant to our audit objectives included control environment, control activities, information and communication, and monitoring. The associated underlying principles significant to our objectives included:

- Board and management commitment to integrity and ethical values.
- Board exercise of oversight responsibility.
- Management evaluation of employee performance and holding individuals accountable for their internal control responsibilities.
- Management design of control activities to achieve the District's objectives and respond to risks.
- Management design of controls over IT.
- Management establishment of policies and procedures to implement internal control activities.
- Management use of relevant and quality information to achieve the District's objectives.
- Management communication of information internally necessary to achieve the District's objectives.
- Management activities to monitor the District's internal control system and evaluate the results.
- Management remediation of identified internal control deficiencies on a timely basis.

This audit was designed to identify, for the IT systems included within the scope of the audit, deficiencies in management's internal controls that were significant to our audit objectives; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or

ineffective operational policies, procedures, or practices. The focus of this audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the IT systems included within the scope of this audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of the audit; obtaining an understanding of and evaluating the IT systems and related significant controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of the audit findings and our conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

This audit included the selection and examination of IT system controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of agency management, staff, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting this audit, we:

- Reviewed applicable laws, rules, Board policies, District procedures, and other guidelines and interviewed District personnel to obtain an understanding of District operations related to PeopleSoft Applications and Focus.
- Obtained an understanding of the District's security management, access, and configuration management controls to protect IT resources.
- Observed, documented, and tested key processes, procedures, and controls related to the District's IT processes for PeopleSoft Applications and Focus infrastructure, including authentication, logical controls, and logging and monitoring of the network and Web and portal servers, application, Web, and database servers, and database management systems; Focus application logical controls and logging and monitoring; data and business process flows within Focus; PeopleSoft Applications and Focus change management; and device management.
- Evaluated the effectiveness of logical access controls, including the periodic reviews of accounts assigned to the network domain and member servers; application, Web, and database servers, and database management systems supporting PeopleSoft Applications and Focus.
- Examined and evaluated the appropriateness of administrative access privileges for the District's member servers as of September 25, 2019, and network domain as of September 16, 2019.
- Examined and evaluated the appropriateness of access privileges granted on the 8 servers supporting PeopleSoft Applications. Specifically, we examined:
    - 58 accounts assigned on the database server supporting the human resources (HR) database and 51 accounts assigned on the database server supporting the finance database as of September 16, 2019.

- 54 accounts assigned to 1 of 4 application servers as of September 19, 2019 and 53 accounts assigned to each of the other 3 application servers as September 16, 2019.
- 52 and 53 accounts assigned to the 2 Web servers as of September 16, 2019.

- Examined and evaluated the appropriateness of access privileges granted on the 31 servers supporting Focus. Specifically, as of September 21, 2019, we examined:
  - 48 accounts assigned to each of the 3 database servers.
  - 50 accounts assigned to each of 17 application and Web servers and 51 accounts assigned to each of the other 3 application and Web servers.
  - 50 accounts assigned to each of the 8 external-facing Web servers.
- Examined and evaluated 12 accounts with administrative access privileges assigned to the HR database and 10 accounts with administrative access privileges assigned to the finance database supporting PeopleSoft Applications, as of September 10, 2019.
- Examined and evaluated the appropriateness of 13 accounts assigned to the database supporting Focus, as of October 3, 2019.
- Evaluated user authentication controls related to the District IT Infrastructure supporting PeopleSoft Applications and Focus.
- For PeopleSoft Applications, examined and evaluated:
  - 5 of the 6 application and Web servers as of September 16, 2019;
  - Root user controls for the 2 database servers as of September 17, 2019; and
  - 1 of the 6 application and Web servers as of September 19, 2019.
- Examined and evaluated 31 application, Web, and database servers supporting Focus as of September 21, 2019.
- Evaluated the effectiveness of logical controls assigned within Focus, including periodic reviews of access privileges.
- Examined and evaluated the appropriateness of access privileges, as of October 3, 2019, granted within Focus for 89 employees and contractors assigned to 16 school-based profiles and 35 employees assigned to 5 system functionality-related profiles.
- Evaluated the effectiveness of District's change management controls related to the authorization, testing, and approval of PeopleSoft Applications and Focus application changes.
- Evaluated the effectiveness of system software and network infrastructure component change control procedures related to the District's IT infrastructure applicable to PeopleSoft Applications and Focus.
- Evaluated the effectiveness of the District's logging and monitoring controls, including actions performed by privileged users, for the infrastructure supporting PeopleSoft Applications and Focus.
- Evaluated the effectiveness of the District's logging and monitoring controls related to student information within Focus.
- Evaluated the effectiveness of controls for vulnerability management related to the IT infrastructure supporting the PeopleSoft Applications and Focus, including secure configurations, vulnerability assessment and remediation, maintenance, monitoring, and analysis of audit logs, and malware defense.
- Evaluated the effectiveness of the District's mobile device security plan, including security and configuration requirements and District- and user-defined responsibilities.

- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe the matters requiring corrective actions. Management's response is included in this report under the heading ***MANAGEMENT'S RESPONSE***.

AUTHORITY

Section 11.45, Florida Statutes, provides that the Auditor General may conduct audits of the IT programs, activities, functions, or systems of any governmental entity created or established by law. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.

Sherrill F. Norman, CPA
Auditor General

MANAGEMENT'S RESPONSE

THE SCHOOL DISTRICT OF PALM BEACH COUNTY, FL

DONALD E. FENNOY II, ED.D.
SUPERINTENDENT

OFFICE OF THE SUPERINTENDENT
3300 FOREST HILL BOULEVARD, C-316
WEST PALM BEACH, FL 33406-5869

PHONE: 561-629-8566 / FAX: 561-649-6837
www.PALMBEACHSCHOOLS.ORG

July 15, 2020

Sherrill F. Norman
Auditor General
Claude Denson Pepper Building, Suite G74
111 West Madison Street
Tallahassee, FL 32399 -1450

Dear Auditor General Norman:

Below is our response to the preliminary and tentative audit findings and recommendations from your IT Operational Audit of the School District of Palm Beach County.

Finding No. 1: Certain District IT security controls need improvement to ensure the confidentiality, integrity, and availability of District data and IT resources.

Recommendation:
We recommend that District management improve IT security controls to ensure the confidentiality, integrity, and availability of District data and IT resources.
Management Response:
Management concurs. District management agrees with the findings and we have taken corrective actions to improve security controls. District IT will continue to improve monitoring and security measures to ensure the confidentiality and security of data stored in District IT systems.

As required, the District's written statement of explanation is submitted electronically in source format with my digitized signature. If you should have any questions or require additional information, please contact Mr. Deepak Agarwal, Chief Information Officer.

Respectfully,

Donald E. Fennoy II, Ed.D.
Superintendent of Schools

cc: Teresa Michael, Inspector General