STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2021-115
January 2021

POLK COUNTY
DISTRICT SCHOOL BOARD

SAP® ENTERPRISE RESOURCE PLANNING SOFTWARE AND FOCUS STUDENT INFORMATION SYSTEM

STATE OF FLORIDA
INTEGRITY INDEPENDENCE OBJECTIVITY
AUDITOR GENERAL

Sherrill F. Norman, CPA
Auditor General

Board Members and Superintendent

During the period, September 2019 through May 2020, Jacqueline M. Byrd served as Superintendent of the Polk County Schools and the following individuals served as School Board Members:

	District No.
Billy Townsend	1
Lori Cunningham, Chair from 11-12-19, Vice-Chair through 11-11-19	2
Sarah Fortney	3
Sara Beth Reynolds	4
Kay Fields	5
Lynn Wilson, Vice Chair from 11-12-19, Chair through 11-11-19	6
Lisa Miller	7

The team leader was Gina Bailey, CPA, CISA, CFE, 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

POLK COUNTY DISTRICT SCHOOL BOARD

SAP® ERP Software and Focus Student Information System

SUMMARY

This operational audit of the Polk County District School Board (District) focused on evaluating selected information technology (IT) controls applicable to the SAP® Enterprise Resource Planning Software (SAP® ERP) and Focus Student Information System (Focus). As summarized below, our audit disclosed areas in which improvements in District controls and operational processes are needed.

Finding 1: The access privileges within Focus for certain employees were unnecessary for the employee's assigned job responsibilities.

Finding 2: Certain District IT security controls related to authentication, vulnerability management, device management, network account management, and logging and monitoring need improvement to ensure the confidentiality, integrity, and availability of District data and IT resources.

BACKGROUND

The Polk 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 Polk County District School Board (Board), which is composed of seven elected members. The appointed Superintendent of Schools is the executive officer of the Board. During the 2019-20 fiscal year, the District operated 133 schools and centers, sponsored 30 charter schools, and reported 136,764 unweighted full-time equivalent students.

The District uses SAP® Enterprise Resource Planning Software (SAP® ERP) 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 IT infrastructure supporting SAP® ERP and Focus, including the network domains, application and database servers, and database management systems.

FINDINGS AND RECOMMENDATIONS

Finding 1: Access Privileges

Access controls are intended to protect data and information technology (IT) resources from unauthorized disclosure, modification, or destruction. Effective access controls include measures that promote an appropriate separation of duties and restrict the access privileges granted to employees and contractors to only those necessary for assigned responsibilities or functions. Such access controls are essential to protect the confidentiality, integrity, and availability of data and IT resources. Appropriately restricted access privileges help protect data and IT resources from unauthorized modification, loss, or disclosure. In addition, documented periodic evaluations of access privileges associated with security roles help ensure that access privileges provided to each security role remain appropriate and necessary.

Access privileges within Focus are controlled by assigning profiles to users. Permissions to access certain modules and to view or edit specific screens and fields are defined to each profile. In addition, documented evaluations of school-level personnel access privileges associated with security roles are periodically conducted; however, similar evaluations for District-level personnel or contractors are not conducted. Our examination of District records for all 73 user accounts assigned the ability to update Districtwide one or more of 9 critical or confidential student data fields related to attendance, grades, classified biographical information,[1] and drug offenses disclosed that 18 accounts, including 15 District-level employee and contractor accounts and 3 test accounts, had unnecessary access privileges to the data fields. Specifically, the Assistant Superintendent of Information Systems and Technology, Director of Information Services, Senior Manager for Instructional Technology Project Implementation, a Senior Database Administrator, and 11 contractors were assigned the system administrator profile which allowed update access to all functions within Focus, including student record origination, correction, and changes to student data.

In response to our inquiry, District management stated that the system administrator profile had been assigned to these individuals based on their responsibility for understanding the functionality of Focus to assist District end users. Notwithstanding this response, each of the employees' and contactors' daily duties did not require complete update access privileges to Focus and such privileges are contrary to an appropriate separation of end-user and technical support functions.

In addition, the individuals assigned the 15 accounts also had access to a test account with Districtwide update access to biographical information and two other test accounts with Districtwide access to biographical information and drug offenses. Although these accounts were used to test functionality of program and profile changes during the implementation of Focus in 2018, these accounts were not in use as of August 2020 and not necessary to have open and available for use beyond monitored testing conditions. According to District management, the District had set up the system to periodically evaluate access privileges associated with security roles of school-level personnel but inadvertently did not establish the evaluations for District-level personnel or contractors.

Appropriately restricting the use and access capabilities of District end users' accounts, consultants' accounts, and accounts used for testing purposes help protect data and IT resources from unauthorized modification, loss, or disclosure. In addition, documented periodic evaluations of assigned user access privileges increase management's assurance that access privileges continue to be appropriate and necessary.

Recommendation: District management should ensure that access granted in Focus is necessary and appropriate for employee and contractor daily duties. To assure the access continues to be appropriate and necessary, District management should also document periodic evaluations of District-level personnel and contractor access privileges.

[1] Classified biographical information includes, for example, student social security numbers, birthdates, ethnicity, gender, and Florida student number.

Finding 2: 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 related to authentication, vulnerability management, device management, network account management, and logging and monitoring 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 related to authentication, vulnerability management, device management, network account management, and logging and monitoring, the risk is increased that the confidentiality, integrity, and availability of District data and related IT resources may be compromised.

Recommendation: District management should improve IT security controls related to authentication, vulnerability management, device management, network account management, and logging and monitoring to ensure the confidentiality, integrity, and availability of District data and IT resources.

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 August 2020 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 our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

This IT operational audit focused on evaluating selected IT controls applicable to SAP® Enterprise Resource Planning Software (SAP® ERP) and Focus Student Information System (Focus) during the period September 2019 through May 2020, and selected actions subsequent thereto. For those areas, 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.
- 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)[2] 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.

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 all internal control components were significant to our audit objectives. The associated underlying principles significant to our objectives included:

- Management establishment of an organizational structure, assignment of responsibility, and delegation of authority to achieve the District's goals and objectives.
- Management design of control activities to achieve the District's objectives and respond to risks.
- Management design of controls over information technology.
- 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 communication of information externally necessary to achieve the District's objectives.

[2] 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.

- 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, regulations, 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 our 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 our 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 our audit findings and 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 vendors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, waste, abuse, or inefficiency.

In conducting our audit, we:

- Reviewed applicable laws, rules, Board policies, District procedures, and other guidelines; interviewed District personnel; and examined District records to obtain an understanding of District operations related to the SAP® ERP and Focus and to evaluate whether District operations were designed properly and operating effectively.
- Evaluated the sufficiency of District controls; observed, documented, and tested key processes, procedures, and controls related to District IT processes for the SAP® ERP and Focus infrastructures, including authentication, logical controls, vulnerability management, logging and monitoring of the network, application, and database servers, database management systems, confidential student records and information, and critical student-related transactions; SAP® ERP and Focus application change management; and device management.
- Evaluated the effectiveness of logical access controls, including the periodic evaluations of accounts assigned to the network domains and member servers; application and database servers; and database management systems supporting the SAP® ERP and Focus.
- Evaluated the effectiveness of logical controls assigned within Focus, including periodic evaluations of assigned user access privileges.

- Examined and evaluated the appropriateness of administrative access privileges for the District's root and child domains as of May 4, 2020, and May 13, 2020, and the member servers as of February 21, 2020.
- Examined and evaluated 447 domain accounts not required to have a password change as of May 7, 2020.
- Examined and evaluated the appropriateness of access privileges granted to the 54 database principles (users, groups, and roles) assigned to the database supporting the SAP® ERP as of February 21, 2020.
- Examined and evaluated the appropriateness of access privileges granted on the database and the four application servers supporting Focus. Specifically, we examined:
  - The 37 accounts assigned to the database server as of May 13, 2020.
  - The 46 accounts assigned to one application server as of May 13, 2020.
  - The 45 accounts assigned to the other three application servers as of May 13, 2020.
- Examined and evaluated the appropriateness of access privileges granted to the 17 accounts assigned to the database supporting Focus as of May 7, 2020.
- Examined and evaluated the appropriateness of access privileges, as of August 12, 2020, granted within Focus for the 73 employees assigned Districtwide update access to one or more of 9 selected confidential or critical student record fields.
- Examined and evaluated the root account and 13 user accounts on the database server and one application server and 12 user accounts on the other three application servers supporting Focus not required to have a password change as of May 13, 2020.
- Evaluated selected security settings related to the SAP® ERP and Focus and the supporting infrastructure to determine whether authentication controls were configured and enforced in accordance with IT best practices.
- Evaluated District procedures related to the SAP® ERP and Focus patches, upgrades, and data fixes to determine whether District change management controls are designed to ensure the appropriate authorization, testing, and approval of the SAP® ERP and Focus changes.
- Examined selected database and server logs to determine the adequacy of District logging and monitoring controls designed for the infrastructure supporting the SAP® ERP and Focus, including actions performed by privileged users.
- Examined selected procedures, logs, and change requests related to the IT infrastructure applicable to the SAP® ERP and Focus to determine whether District system software and network infrastructure component change control procedures were designed in accordance with IT best practices.
- Evaluated District procedures related to recording, documenting, and reporting changes to confidential and critical student record information within Focus to determine the adequacy of the District's logging and monitoring controls.
- Examined selected scan reports, audit policies, logs, and documents to evaluate the adequacy of the District's controls for vulnerability management related to the IT infrastructure supporting the SAP® ERP and Focus, including secure configurations, vulnerability assessment and remediation, maintenance, monitoring, and analysis of audit logs, and malware defense.
- Evaluated procedures related to the District mobile device security plan, including security and configuration requirements, to determine the adequacy of controls for managing mobile devices connected to the District's network or used to store confidential and sensitive data.

- 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.

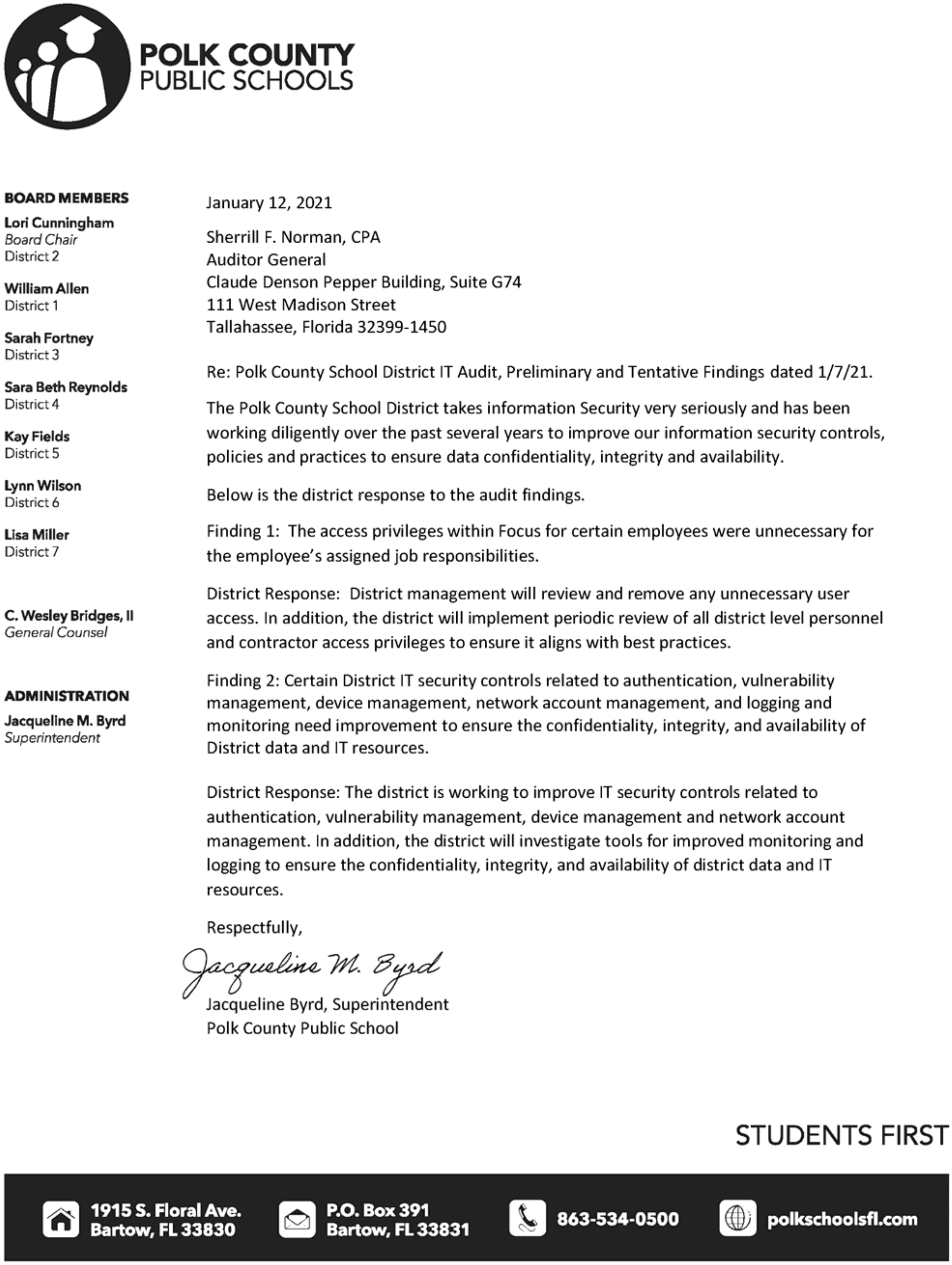
AUTHORITY

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

Sherrill F. Norman, CPA
Auditor General

MANAGEMENT'S RESPONSE



POLK COUNTY
PUBLIC SCHOOLS

January 12, 2021

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

Re: Polk County School District IT Audit, Preliminary and Tentative Findings dated 1/7/21.

The Polk County School District takes information Security very seriously and has been working diligently over the past several years to improve our information security controls, policies and practices to ensure data confidentiality, integrity and availability.

Below is the district response to the audit findings.

Finding 1: The access privileges within Focus for certain employees were unnecessary for the employee's assigned job responsibilities.

District Response: District management will review and remove any unnecessary user access. In addition, the district will implement periodic review of all district level personnel and contractor access privileges to ensure it aligns with best practices.

Finding 2: Certain District IT security controls related to authentication, vulnerability management, device management, network account management, and logging and monitoring need improvement to ensure the confidentiality, integrity, and availability of District data and IT resources.

District Response: The district is working to improve IT security controls related to authentication, vulnerability management, device management and network account management. In addition, the district will investigate tools for improved monitoring and logging to ensure the confidentiality, integrity, and availability of district data and IT resources.

Respectfully,

Jacqueline M. Byrd

Jacqueline Byrd, Superintendent
Polk County Public School

STUDENTS FIRST