STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2020-053
November 2019

ST. JOHNS COUNTY DISTRICT SCHOOL BOARD

PowerSchool Unified Administration™ BusinessPlus and PowerSchool eSchoolPlus Student Information System

Sherrill F. Norman, CPA
Auditor General

Board Members and Superintendent

During the period October 2018 through July 2019, Tim Forson served as Superintendent of the St. Johns County Schools and the following individuals served as School Board Members:

	District No.
Beverly Slough, Vice Chair	1
Tommy Allen	2
Bill Mignon	3
Kelly Barrera, Chair	4
Patrick Canan	5

The team leader was Vikki Mathews, 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

ST. JOHNS COUNTY DISTRICT SCHOOL BOARD

PowerSchool Unified Administration™ BusinessPlus and PowerSchool eSchool Plus Student Information System

SUMMARY

This operational audit of St. Johns District School Board (District) focused on evaluating selected information technology (IT) controls applicable to the PowerSchool Unified Administration™ BusinessPlus (BusinessPlus) and the PowerSchool eSchoolPlus Student Information System (eSchoolPlus) for managing and reporting the District's finance, human resources, and student transactions and information, and the supporting infrastructure for each system. As summarized below, our audit disclosed areas in which improvements in District controls and operational processes are needed:

Finding 1: Some District employees' access privileges granted within eSchoolPlus were unnecessary for the employees' assigned job responsibilities.

Finding 2: District controls related to periodic reviews of access to the servers and databases and network administrator groups need improvement.

Finding 3: District IT security controls related to user authentication, user account management, logging and monitoring, and vulnerability management need improvement to ensure the confidentiality, integrity, and availability of District data and IT resources.

BACKGROUND

The St. Johns County School District (District) is a 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 St. Johns County District School Board (Board), which is composed of five elected members. The appointed Superintendent of Schools is the executive officer of the Board. During the 2018-19 fiscal year, the District had 49 centers and schools other than charter schools, 3 charter schools, and reported 45,401 unweighted full-time equivalent students.

The District uses PowerSchool Unified Administration™ BusinessPlus (BusinessPlus) to process and report finance and human resources information and PowerSchool eSchoolPlus Student Information System (eSchoolPlus) to process and report student information. In addition, the District maintains and manages the information technology infrastructure supporting BusinessPlus and eSchoolPlus, including the network domain, application and database servers, and database management systems.

FINDINGS AND RECOMMENDATIONS

Finding 1: Appropriateness of 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 restrict the

access privileges granted to employees 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.

Employees are granted access privileges to transactions and information within eSchoolPlus through assigned roles. As part of our audit procedures, we identified 11 roles that allowed access to District defined confidential and sensitive data. Our examination of the access privileges for all 259 eSchoolPlus users assigned 1 or more of the 11 roles indicated that some employees' access to selected student information were unnecessary. Specifically:

- One Medicaid Specialist, one Executive Secretary for Guidance and Choice, the Coordinator of School Services, and one Executive Secretary of School Services had the ability to update information regarding contact with students concerning social services. In addition, two programmer analysts had the ability to view students' free and reduced lunch status and one Executive Secretary of School Services had the ability to update information regarding student mental health services. These access privileges were not necessary for the employees' assigned responsibilities. Subsequent to our inquiry, District management indicated that the access privileges were reduced or removed for these employees.
- The District assigned 86 employees, including principals, assistant principals, registrars, computer operators, and confidential secretaries, a role that allowed the assumption of other employees' granted access privileges, allowing an employee to act as another employee within the system. Subsequent to our inquiry, District management indicated that this role was removed from all 86 employees.

Assigning access privileges to sensitive or confidential functions within the eSchoolPlus system that are not required for the employee's job responsibilities increases the risk of unauthorized modification, loss, or disclosure of data and IT resources.

Recommendation: We recommend that District management continue efforts to restrict employee access privileges granted within eSchoolPlus to only those necessary for the employee's assigned responsibilities.

Finding 2: Periodic Review of Access Privileges

Effective access controls include periodic reviews of accounts and associated access privileges to data and IT resources to help ensure that only authorized accounts have access and that access provided to each account remains appropriate and necessary.

Our audit procedures disclosed that District management had not established procedures for, and had not performed, periodic reviews of all groups and accounts (i.e., staff, system, and service accounts) and associated privileges on the Windows servers and databases supporting BusinessPlus and eSchoolPlus, or of all privileged accounts used to manage the District's network domain. Subsequent to our inquiry District management indicated that quarterly reviews of access privileges for groups and accounts on the servers and databases and administrator groups on the network would be implemented.

Periodic reviews of groups and accounts and associated privileges increase management's assurance that accounts continue to be authorized and appropriate and reduce the risk that unauthorized disclosure, modification, or destruction of District data and IT resources may occur.

Recommendation: We recommend that District management establish procedures for, and perform and document, periodic reviews of all groups and accounts and the associated privileges on the Windows servers and databases, and of all privileged accounts used to manage the District's network domain.

Finding 3: Security Controls – User Authentication, User Account Management, Logging and Monitoring, and Vulnerability Management.

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 user authentication, user account management, logging and monitoring, and vulnerability management 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 specific issues.

Without appropriate security controls related to user authentication, user account management, logging and monitoring, and vulnerability management, the risk is increased that the confidentiality, integrity, and availability of District data and IT resources may be compromised.

Recommendation: We recommend that District management improve IT security controls related to user authentication, user account management, logging and monitoring, and vulnerability management 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 February 2019 through July 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 St. Johns County District School Board IT controls applicable to PowerSchool Unified Administration™ BusinessPlus (BusinessPlus) and PowerSchool eSchoolPlus Student Information System (eSchoolPlus) during the period October 2018 through May 2019 and selected actions thereto. The overall objectives of the audit 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 identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

This audit was designed to identify, for the IT systems and controls included within the scope of the audit, deficiencies in management's internal controls; 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 and controls 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 the IT systems and 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.

In conducting this audit, we:

- Interviewed District staff and reviewed District documentation to obtain an understanding of and evaluate District operations for BusinessPlus and eSchoolPlus and the supporting IT infrastructure, including authentication, logical controls, change management, vulnerability management, and logging and monitoring of the network, application and database servers, and the database management systems; eSchoolPlus application logical controls, change management, and logging and monitoring; and the data and business process flows within eSchoolPlus.
- Evaluated the effectiveness of logical access controls, including periodic reviews of access privileges assigned within eSchoolPlus.
- Evaluated the effectiveness of logical access controls, including periodic reviews of accounts assigned to the network domain, database management systems, and servers supporting BusinessPlus and eSchoolPlus.
- Examined and evaluated the appropriateness of administrative privileges for the District's network domain, as of March 7, 2019, and for selected servers supporting BusinessPlus and eSchoolPlus, as of March 13, 2019.
- Examined and evaluated 81 database principals (users, groups, and roles) assigned to the database supporting BusinessPlus, as of February 28, 2019, and 99 database principals assigned to the database supporting eSchoolPlus, as of March 5, 2019.
- Examined and evaluated the appropriateness of access privileges, as of April 18, 2019, granted within eSchoolPlus for 259 employees.
- Evaluated user authentication controls related to the District's IT infrastructure supporting BusinessPlus and eSchoolPlus.

- Evaluated the effectiveness of District's change management controls related to the authorization, testing, and approval of BusinessPlus and eSchoolPlus application changes.
- Evaluated the effectiveness of system software and network infrastructure component change control procedures related to the District's IT infrastructure applicable to BusinessPlus and eSchoolPlus.
- Evaluated the effectiveness of the District's logging and monitoring controls, including actions performed by privileged users, for the network domain and servers and databases supporting BusinessPlus and eSchoolPlus.
- Evaluated the effectiveness of the District's logging and monitoring controls related to student information within eSchoolPlus.
- Evaluated the effectiveness of controls for vulnerability management related to the IT infrastructure supporting the BusinessPlus and eSchoolPlus, including secure configurations, vulnerability assessment and remediation, maintenance, monitoring, and analysis of audit logs, and malware defense.
- 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

Tim Forson
Superintendent of Schools

40 Orange Street
St. Augustine, Florida 32084
(904) 547-7500
www.stjohns.k12.fl.us

November 5, 2019

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

Re: St. Johns County School District IT Audit, Preliminary and Tentative Findings dated 10/23/2019

The St Johns County School District takes Information Security very seriously and works each year to continually improve our information security controls, policies and practices to ensure data confidentiality, integrity and availability.

Our response to each of the audit findings are noted below:

Finding 1: Some District employees' access privileges granted within eSchoolPlus were unnecessary for the employees' assigned job responsibilities.
District Response 1: We have removed the unnecessary user accounts and established new practices to review this access quarterly.

Finding 2: District controls related to periodic reviews of access to the servers and databases and network administrator groups need improvement.
District Response 2: We have implemented a quarterly review of privileged accounts on servers, databases and administrative groups.

Finding 3: District IT security controls related to user authentication, user account management, logging and monitoring, and vulnerability management need improvement to ensure the confidentiality, integrity, and availability of District data and IT resources.
District Response 3: We are working to improve security controls related to user authentication, account management, logging, and vulnerability management to improve our overall information security posture.

If you have any questions, please contact Bruce Patrou, Chief Information Officer, at (904) 547-3920.

Sincerely,

Tim Forson

Tim Forson, Superintendent
St. Johns County School District

cc: Cathy Mittelstadt, Deputy Superintendent for Operations
Bruce Patrou, Chief Information Officer

The St. Johns County School District will inspire good character and a passion for lifelong learning in all students, creating educated and caring contributors to the world.