STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2022-034
October 2021

ORANGE COUNTY DISTRICT SCHOOL BOARD

SAP® ENTERPRISE RESOURCE PLANNING SOFTWARE AND SKYWARD STUDENT INFORMATION SYSTEM

Sherrill F. Norman, CPA
Auditor General

Board Members and Superintendent

During the period, September 2019 through December 2020, Dr. Barbara Jenkins served as Superintendent of the Orange County Schools and the following individuals served as School Board Members:

	District No.
Teresa Jacobs, Chair	Districtwide
Angie Gallo	1
Johanna López	2
Linda Kobert	3
Pam Gould, Vice-Chair from 11-13-19	4
Kathleen "Kat" Gordon through 11-16-20, Vice-Chair through 11-12-19	5
Vicki-Elaine Felder from 11-17-20	5
Dr. Karen Castor Dentel	6
Melissa Byrd	7

The team leader was Sue Graham, CPA, 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

ORANGE COUNTY DISTRICT SCHOOL BOARD

SAP® Enterprise Resource Planning Software and Skyward Student Information System

SUMMARY

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

Finding 1: District controls over application security management need improvement to ensure that access privileges to student information granted within Skyward are necessary and appropriate.

Finding 2: District IT security controls over user authentication, account management, monitoring, and vulnerability management need improvement to ensure the confidentiality, integrity, and availability of District data and IT resources.

BACKGROUND

The Orange 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 Orange County District School Board (Board), which is composed of eight elected members. The appointed Superintendent of Schools is the executive officer of the Board. During the 2020-21 fiscal year, the District operated 222 schools and centers, sponsored 41 charter schools, and reported 244,502 unweighted full-time equivalent students.

The District uses the SAP® Enterprise Resource Planning Software (SAP® ERP) to process and report finance and human resources transactions and the Skyward Student Information System (Skyward) for the recording, processing, and reporting of student record information. In addition, the District maintains and manages the application and database servers and database management system supporting the SAP® ERP.

FINDINGS AND RECOMMENDATIONS

Finding 1: Application Security Management

Access controls are intended to protect data and information technology (IT) resources from unauthorized disclosure, modification, or destruction. Effective access controls include granting employees access to IT resources based on a demonstrated need to view, change, or delete data and restricting employees from performing incompatible functions or functions outside of their areas of responsibility. In addition, documented periodic evaluations of access privileges associated with security groups help ensure that access privileges provided to each security group remain appropriate and necessary.

Access privileges within Skyward are controlled by assigning module or function-based security groups to users. Permission to view or edit specific screens and fields are defined to each security group. Security groups are defined at the District level or at the school level allowing employees to be assigned access privileges across the District or at one or more schools and are additionally defined to allow inquiry or update access privileges to a specific function such as grades or attendance. Update access privileges within Skyward may also be granted to all functions through the assignment of Systemwide access, including student module Systemwide access (i.e., record origination, correction, and changes to student data) and product setup module Systemwide access (i.e., security tables, configuration files, and utilities). Our audit procedures disclosed that the District's management of Skyward user access privileges needs improvement. Specifically:

- Through inquiry with District personnel and examination of District records, we identified five security groups that allowed Districtwide update access privileges to student attendance, discipline, grades, graduation requirements, and health records, respectively. Our examination of the access privileges for 13 of the 55 District employees assigned one or more of the five security groups as of November 2020 disclosed that:

    - 4 employees, an area administrator, an executive secretary, the Executive Director of Exceptional Student Education, and the Director of Data Strategy, had unnecessary Districtwide update access to student discipline records, although the employees assigned responsibilities only required Districtwide inquiry access. Additionally, the Director of Data Strategy had unnecessary Districtwide update access to student attendance records.
    - An administrative specialist retained Districtwide update access to student attendance records while on extended medical leave and unable to perform her assigned responsibilities.
    - A college transition counselor had update access to student grade and graduation requirement records Districtwide instead of to only those schools needed for her assigned responsibilities.

  In response to our inquiry, District management indicated that the employee on medical leave retained her access in accordance with the District's standard practice and that the other 5 employees' unnecessary access resulted from either a lack of defined security groups granting inquiry-only access to functions Districtwide, or errors made in the level of access requested. Subsequent to our inquiry, District management indicated that Districtwide update access was removed for the 5 employees and a security group that allows Districtwide inquiry-only access to discipline records was created and assigned to the appropriate users.

- Our examination of all Systemwide access privileges granted as of November 2020 disclosed that 15 District personnel had been granted student module Systemwide access and 19 District personnel had been granted both student module Systemwide access and product setup module Systemwide access. District personnel granted Systemwide access privileges included developers, application analysts, and specialists for student systems; District consultants and other IT Services employees; directors, developers, and business analysts within the Division of Teaching and Learning; business analysts for Curriculum and Digital Learning; a teacher; and the Director for State Reporting.

  In response to our inquiry regarding the number of District personnel having the level of access capabilities granted through Systemwide access privileges, District management indicated that the teacher's access privileges were no longer necessary but had not been timely requested for removal. The access privileges assigned to the other District personnel were for ongoing Skyward project team responsibilities, including analysis of business and user needs, translation of process changes into system requirements and specifications, and the technical configuration of Skyward. In addition, access to some screens within Skyward necessary to perform specific tasks was not available to these personnel through the District's defined security groups. Notwithstanding the need for some personnel to have Systemwide access to perform tasks necessary for the configuration, maintenance, and support of the Skyward application, accounts with such access should be limited to the least number possible as full update access to all student data is contrary to an appropriate separation of end-user and technical support functions.

- District management had not performed a documented evaluation of access privileges granted within Skyward since implementation of the system in July 2019. Although District management indicated that an automated process for changing or removing access privileges for transferred or terminated employees was in place, and an annual evaluation of access to social security numbers was performed, these procedures were not sufficient to ensure the appropriateness of all access privileges granted to school-based employees within Skyward. In response to our inquiry, District management indicated that, for Systemwide access, a monthly report would be developed for the evaluation and timely removal of employee access privileges.

Appropriately restricted access privileges help protect District data and IT resources from unauthorized modification, loss, and disclosure. In addition, documented periodic evaluations provide assurance that granted access privileges remain appropriate and necessary.

Recommendation: District management should promptly conduct a documented evaluation of the access privileges granted within Skyward to verify that the privileges are necessary and appropriate for each user's assigned responsibilities. In addition, District management should enhance procedures to ensure that documented periodic evaluations are conducted to verify that the access privileges continue to be necessary and appropriate.

Finding 2: Security Controls – User Authentication, Account Management, 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, account management, monitoring, and vulnerability management needed 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 user authentication, account management, monitoring, and vulnerability management, 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 user authentication, account management, 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 September 2020 through July 2021 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 the SAP® Enterprise Resource Planning Software (SAP® ERP) and Skyward Student Information System (Skyward) during the period September 2019 through December 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.
- 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 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 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 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, 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 Skyward 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 infrastructure and Skyward, including authentication, logical controls, vulnerability management, and logging and monitoring of network events, the SAP® ERP database server and database management system, confidential student records and information, and critical student-related transactions.
- Evaluated the effectiveness of logical controls assigned within Skyward, including Systemwide access, and periodic evaluations of assigned user access privileges.
- Examined and evaluated the appropriateness of access privileges granted within Skyward for 13 of the 55 employees assigned Districtwide update access to one or more of five selected confidential or critical student security groups as of November 3, 2020.
- Examined and evaluated the appropriateness of Skyward Systemwide access privileges granted for all 34 District personnel accounts as of November 3, 2020.
- Evaluated District change management controls, including authorization, testing, and approval using the Skyward change utility.
- Evaluated District procedures and reviewed reports related to the recording, documenting, and reporting of changes to selected confidential and critical student record information within Skyward to determine the adequacy of District logging and monitoring controls over student information.
- Evaluated selected security settings related to the database server and database supporting the SAP® ERP and selected network devices to determine whether authentication controls were configured and enforced in accordance with IT best practices.
- Examined and evaluated the appropriateness of password changes, as of October 9, 2020, for the four active accounts assigned to the database and the seven active accounts assigned to the database server supporting the SAP® ERP.
- Evaluated the effectiveness of logical access controls, including the periodic evaluations of accounts assigned to the database server and database supporting the SAP® ERP.
- Examined and evaluated the appropriateness of access privileges granted to the 33 accounts on the database server supporting the SAP® ERP as of October 9, 2020.
- Examined and evaluated the appropriateness of the 8 accounts assigned selected administrative privileges for the database supporting the SAP® ERP as of October 9, 2020.
- Examined selected database and server logs to determine the adequacy of District logging and monitoring controls designed for the infrastructure supporting the SAP® ERP, including actions performed by privileged users.
- Examined and evaluated the appropriateness of the 11 accounts assigned to the District-managed firewall as of October 9, 2020.
- Evaluated the effectiveness of District configuration management controls for selected network devices and the database server and database supporting the SAP® ERP, including establishing, modifying, and monitoring standard secure configurations and implementing software updates.
- Evaluated the effectiveness of controls over administrative access to computers on the District network.

- Evaluated the effectiveness of controls over end-of-life management for District servers.
- Examined selected logs, alert messages, and documents to evaluate the adequacy of District vulnerability management controls, including policies and procedures for scanning, analysis, and remediation of identified vulnerabilities; regular penetration testing; appropriate tools for identification of malicious software; and malware defense; and logging and monitoring of network events, including selected network devices.
- 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

Orange County
Public Schools

445 W. Amelia Street• Orlando, Florida 32801 • (407) 317-3200 • www.ocps.net

October 19, 2021

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

Re: Information Technology Operational Audit of the Orange County District School Board, SAP ERP Software and Skyward Student Information System

Dear Ms. Norman:

Per your letter dated September 22, 2021, the following represents our responses to the findings noted.

Finding No. 1: Application Security Management

Response: To ensure access privileges to Skyward remain appropriate and necessary, the following procedures have been implemented:

1) A monthly review of the staff who have full access to the Student Management suite of modules, and/or System Wide Access was implemented in February 2021. A report of the users with this access is run from Skyward and provided to the Skyward Project Team and District IT leadership to review. Removal of access is then completed if a change is determined. This is in addition to the automated process that removes Skyward security when a user changes work location or job title.
2) A new process will be implemented in October 2021 for the annual review of access privileges of school and district users of Skyward.
    a. For school-based staff, principals will complete a survey to indicate that they have reviewed their Skyward users and their access to the data at their school. Their response to the survey indicates either that they approve of the users' access, or that they have completed a request to have users' access modified - if it is no longer necessary or appropriate.

For district-based staff, Business Process Owners (BPO-district department leaders who are responsible for different areas of student data) will complete a survey to indicate that they have reviewed the Skyward users who are in the Skyward security groups that can modify data in the

"The Orange County School Board is an equal opportunity agency."

area/s of the system the BPO is responsible for. The reports of users with access to the security group/s is run from Skyward and then provided to the Business Process Owner in a secure location for their review. Their response to the survey indicates either that they approve of the users' access, or that they have completed a request to have users' access modified - if it is no longer necessary or appropriate.

Finding No. 2: Security Controls - User Authentication,Account Management, Monitoring, andVulnerability Management

Response: The OCPS ITS Department has reviewed and agrees with the findings of the Auditor General stating that certain security controls related to user authentication, account management, monitoring, and vulnerability management needed improvement. While some findings have been addressed, others are being reviewed for proper resolutions.

Respectfully submitted,

Barbara M. Jenkins, Ed.D
Superintendent

C: Robert Curran, Chief Information Officer, OCPS
Linda Lindsey, School Board Internal Auditor, OCPS
OCPS School Board