STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2023-194
June 2023

LAKE COUNTY DISTRICT SCHOOL BOARD

Skyward School Business Suite and Student Management Suite Software

Sherrill F. Norman, CPA
Auditor General

Board Members and Superintendent

During the period January 2022 through December 2022, Diane S. Kornegay served as Superintendent of the Lake County Schools and the following individuals served as School Board Members:

	District No.
Bill Mathias	1
Tyler Brandeburg from 6-13-22	2
Dr. Kristi Burns through 6-12-22	2
Marc Dodd, Chair from 11-28-22, Vice Chair through 11-27-22	3
Mollie Cunningham, Vice Chair from 11-28-22	4
Stephanie Luke, Chair through 11-27-22	5

The team leader was Joseph Clayton 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

LAKE COUNTY DISTRICT SCHOOL BOARD

Skyward School Business Suite and Student Management Suite Software

SUMMARY

This operational audit of Lake County School District (District) focused on evaluating selected information technology (IT) controls applicable to the Skyward school business suite and student management suite software and District IT infrastructure, and included a follow-up on findings noted in our report No. 2018-024. Our audit disclosed the following:

Finding 1: Certain District IT security controls related to user authentication, account management, data recovery, vulnerability management, and configuration management need improvement to ensure the confidentiality, integrity, and availability of District data and IT resources.

BACKGROUND

The Lake County School District (District) is part of the State system of public education under the general direction of the Florida Department of Education and is governed by State law and State Board of Education rules. Geographic boundaries of the District correspond with those of Lake County. The governing body of the District is the Lake 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 2021-22 fiscal year, the District operated 48 elementary, middle, high, and specialized schools; sponsored 12 charter schools; and reported 52,496 unweighted full-time equivalent students.

The District uses the Skyward school business suite software and student management suite software (Skyward) to process and report financial, human resources, and student information. In addition, the District maintains and manages the network domains and supporting infrastructure (i.e., network domains, operating systems, and database management systems) for Skyward.

Finding 1: Security Controls – User Authentication, Account Management, Data Recovery, Vulnerability Management, and Configuration 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, data recovery, vulnerability management, and configuration 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 the five findings in the areas needing improvement. Similar findings related to user authentication and account management were noted in our report No. 2018-024.

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

Recommendation: District management should improve the IT security controls related to user authentication, account management, data recovery, vulnerability management, and

configuration management to ensure the confidentiality, integrity, and availability of District data and IT resources.

PRIOR AUDIT FOLLOW-UP

Except as discussed in Finding 1, the District had taken corrective actions for the findings included in our report No. 2018-024.

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 information technology (IT) operational audit from September 2022 through April 2023 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 IT controls applicable to the Skyward school business suite and student management suite software (Skyward) and District infrastructure during the period January 2022 through December 2022 and selected actions subsequent thereto. For those areas addressed by this audit, our audit objectives were:

- To determine the effectiveness of selected significant IT controls in achieving management's 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 our report No. 2018-024.
- 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, 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, waste, abuse, or inefficiency.

In conducting this audit, we:

- Reviewed applicable laws, rules, and other guidelines to obtain an understanding of District organizational structure and regulatory requirements; reviewed District procedures, interviewed District personnel, and examined District records to obtain an understanding of District operations related to Skyward and IT infrastructure 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 Skyward and the District IT infrastructure, including authentication, change management, backup and recovery, configuration of systems, logical controls, and inventory and vulnerability management.
- Examined selected security settings related to the District network infrastructure, externally facing applications, remote access systems, and other critical servers and devices to determine whether authentication controls were configured and enforced in accordance with IT best practices, including the use of multi-factor authentication.
- Evaluated the effectiveness of District logical access controls assigned to the District network and selected network devices, including the periodic evaluation of assigned accounts.
- Examined and evaluated the appropriateness of all accounts assigned administrator access privileges, as of September 9, 2022, within the four default network administrator system groups for the District network domains.
- Examined and evaluated, as of September 9, 2022, 33 of the 113 accounts on the root domain and 1 child domain not required to have a password change.
- Examined and evaluated the appropriateness of all accounts assigned administrator access privileges, as of September 9, 2022, for the two District high-risk network devices.
- Examined and evaluated selected District patch management controls for operating systems and network devices to ensure secure configurations are maintained. Specifically, we examined and evaluated the patch management controls for:
    - 32 critical servers as of September 9, 2022, and the additional 6 critical servers as of October 25, 2022.
    - The 2 high-risk network devices as of September 9, 2022.
- Evaluated District procedures and examined selected backup reports to determine the adequacy of the District data recovery procedures to restore District IT assets to a pre-incident trusted state.

- Evaluated the effectiveness of District configuration management controls, including establishing and maintaining secure configurations; disabling insecure protocols; implementing firewalls or port filtering to protect network resources; and timely applying software updates and managing device end-of-life.
- Evaluated District procedures and examined selected records to determine the adequacy of District procedures for maintaining a software asset inventory and ensuring only authorized software is installed on the network.
- Evaluated District procedures and examined selected scan reports and policies to evaluate the adequacy of District vulnerability management controls related to the IT infrastructure, including vulnerability assessment and remediation, malicious software identification, and malware defense.
- Examined and evaluated the appropriateness of administrative access privileges to the one application server, two Web servers, and two database servers that support Skyward as of September 9, 2022.
- Evaluated the effectiveness of District change management controls related to the authorization, testing, and approval of Skyward application data changes prior to implementation into the production environment. Specifically, we examined the four data changes for the school business suite and the one data change for the student management suite logged between October 1, 2021, and August 15, 2022.
- Evaluated the effectiveness of the District security awareness training program.
- Evaluated District procedures and examined select District records to determine the adequacy of District change management procedures related to Skyward.
- Evaluated District controls in place for the use of systemwide access privileges.
- 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

LAKE COUNTY SCHOOLS

201 West Burleigh Boulevard · Tavares · FL 32778-2496
(352) 253-6500 · Fax: (352) 253-6503 · *www.lake.k12.fl.us*

Superintendent:
Diane S. Kornegay, M.Ed.

School Board Members:
District 1
Bill Mathias
District 2
Tyler Brandeburg
District 3
Marc Dodd
District 4
Mollie Cunningham
District 5
Stephanie Luke

June 5, 2023

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

Dear Ms. Norman:

First, we would like to thank you and your staff for the professional manner in which the audit was conducted. We look to the audit process as a valuable tool in our continuous improvement of the IT related operations of our school district.

We have reviewed the list of preliminary and tentative audit findings and recommendations related to the IT operational/security audit of the District and present our specific responses below:

Preliminary and Tentative Finding 1: Security Controls - User Authentication, Account Management, Data Recovery, Vulnerability Management, and Configuration Management

Recommendation: District management should improve the IT security controls related to user authentication, account management, data recovery, vulnerability management, and configuration management to ensure the confidentiality, integrity, and availability of District data and IT resources.

District Response: Lake County Schools acknowledges the findings cited in the audit report and is actively working on remediating the areas listed above.

If you have any questions about the district response to the IT Operational/Security Audit, please contact Duane Weeks, Chief Technology Officer for Lake County Schools at (352) 253-6710 or weeksd@lake.k12.fl.us.

Sincerely,

Diane S Kornegay

Diane S. Kornegay, M.Ed.
Superintendent
Lake County Schools