STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2026-181
June 2026

LEON COUNTY
DISTRICT SCHOOL BOARD

Skyward School Business Suite and Focus Student Information System

Sherrill F. Norman, CPA
Auditor General

Board Members and Superintendent

During the period February 2025 through January 2026, Rocky Hanna served as Superintendent of the Leon County Schools and the following individuals served as School Board members:

	District No.
Alva Swafford Smith	1
Rosanne Wood	2
Darryl Jones, Vice Chair from 11-18-25	3
Laurie Lawson Cox, Chair through 11-17-25	4
Dr. Marcus Nicolas, Chair from 11-18-25, Vice Chair through 11-17-25	5

The Auditor General conducts audits of government 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.

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

LEON COUNTY DISTRICT SCHOOL BOARD

Skyward School Business Suite and Focus Student Information System

SUMMARY

This operational audit of Leon County School District (District) focused on evaluating selected information technology (IT) controls applicable to the Skyward School Business Suite and Focus Student Information System and District IT infrastructure, and included a follow-up on findings noted in our report No. 2020-156. Our audit disclosed the following:

Finding 1: District controls over application security management need improvement to ensure that assigned user access privileges remain necessary and appropriate.

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

BACKGROUND

The Leon 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 Leon County. The governing body of the District is the Leon County District School Board (Board), which is composed of five elected members. The elected Superintendent of Schools is the Executive Officer of the Board. During the 2024-25 fiscal year, the District operated 49 elementary, middle, high, and specialized schools; sponsored 5 charter schools; and reported 36,722 unweighted full-time equivalent students.

The District uses the Skyward School Business Suite (Skyward) to process and report financial and human resource information and the Focus Student Information System (Focus) to process and report student information. Application service provider, Integrated Systems Corporation, and software vendor, Focus School Software, host the applications and maintain and manage the supporting application and database infrastructure for Skyward and Focus, respectively. The District maintains and manages the network domains and IT infrastructure supporting access to Skyward and Focus.

FINDINGS AND RECOMMENDATIONS

Finding 1: Application Security Management

Effective application security management provides a framework for managing risk, developing policies, and monitoring the adequacy of application-related controls. These controls include granting access to information technology (IT) resources based on a demonstrated need to view, change, or delete data and restricting employees from performing incompatible functions or functions beyond their areas of responsibility. Periodic evaluations of access privileges assigned to employees are necessary to ensure

that employees can access only those IT resources that are necessary to perform their assigned job duties and that the assigned access privileges enforce an appropriate separation of incompatible duties.

According to Technology and Information Services Department personnel, the Department maintains a record of school principal and department supervisor-requested and approved employee access privilege changes for Focus Student Information System (Focus) and Skyward School Business Suite (Skyward). The Department is also responsible for providing reports of access privilege assignments to school principals and department supervisors to annually conduct comprehensive access privilege evaluations and confirmations to determine whether the assignments remain appropriate or should be modified.

As part of our audit, we requested for examination District records demonstrating the District's most recent comprehensive evaluation of Focus and Skyward access privileges. We found that District procedures had not been established to ensure that the annual comprehensive evaluation and confirmation process was promptly and effectively completed. Specifically, District records indicated that:

- During the 2024-25 fiscal year, 48 school principals were responsible for evaluating and confirming the assigned Focus access privileges of 2,586 employees. While District records documented approved access privilege changes for Focus, District records did not demonstrate that the Department sent reports to the school principals to evaluate and confirm all Focus access privileges and records did not demonstrate that school principals or other District personnel conducted comprehensive access privilege evaluations of the 2,586 employees during that fiscal year.
- In July 2025, Department personnel requested that the 69 school principals and department supervisors evaluate and confirm, by August 2025, whether the privileges of the 422 employees with access to Skyward remained appropriate. While District records documented approved access privilege changes for Skyward, District records as of May 2026 did not demonstrate that 11 principals and supervisors or other District personnel had conducted comprehensive Skyward access privilege evaluations of 69 individuals for propriety.

In response to our inquiry, District management indicated that, beginning July 2026, the Focus and Skyward access evaluations would require written certification from school principals and department supervisors to confirm whether access privileges remain appropriate or should be modified. Effective, documented, periodic evaluations of assigned access privileges help support whether employee access should continue or be modified and reduce the risk that unauthorized disclosure, modification, or destruction of District IT resources and data may occur.

Recommendation: District management should establish effective procedures for documenting annual evaluations of access privilege assignments for Focus and Skyward and whether the privileges continue to be appropriate or should be modified.

Finding 2: Security Controls – User Authentication, Account Management, and Data Recovery

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, and data recovery 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 three findings in the areas needing improvement.

Without appropriate security controls related to user authentication, account management, and data recovery, the risk is increased that the confidentiality, integrity, and availability of District data and related IT resources may be compromised. A similar finding related to account management was noted in our report No. 2020-156.

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

PRIOR AUDIT FOLLOW-UP

Except as discussed in Finding 2, the District had taken corrective actions for the findings included in our report No. 2020-156.

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 2025 through April 2026 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 cybersecurity controls designed to prevent, detect, or mitigate security risks to the District IT environment, including the critical network infrastructure supporting access to Skyward School Business Suite (Skyward) and Focus Student Information System (Focus), during the period February 2025 through January 2026 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. 2020-156.
- 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 the District organizational structure and regulatory requirements, and reviewed District procedures, interviewed District personnel, and examined District records to obtain an understanding of District operations related to Skyward and Focus and IT infrastructure and to evaluate whether District operations were designed properly and operating effectively.
- Evaluated selected security settings related to Skyward and Focus and the District network infrastructure to determine whether authentication controls were configured and enforced in accordance with best practices.
- Evaluated the effectiveness of District logical access controls assigned to the District network and selected network devices, including the periodic evaluation of assigned user and administrator access privileges.
- Evaluated the effectiveness of logical access controls for Skyward and Focus, including District procedures for the periodic evaluation of assigned user access privileges.
- Examined and evaluated the appropriateness of all accounts assigned administrator access privileges for Focus as of October 17, 2025.
- Examined and evaluated the appropriateness of all accounts assigned administrator access privileges, as of October 6, 2025, within the four default network administrator system groups for the District forest and grandchild network domains.
- Examined and evaluated the appropriateness of all accounts assigned administrator access privileges, as of October 6, 2025, for the District's two high risk network devices.
- 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 District records to evaluate the effectiveness of District configuration management controls, including establishing and maintaining secure configurations; disabling insecure protocols; implementing firewalls to protect network resources; and timely applying software patches and updates and managing device end-of-life.
- Examined and evaluated selected District patch management controls for operating systems and network devices to ensure that secure configurations are maintained. Specifically, we examined and evaluated:
  - As of January 30, 2026, the 5 operating system versions installed for District devices.
  - As of February 5, 2026, the 2 high risk network devices for the District network.
  - As of March 3, 2026, the 27 critical servers for the District network.
- Evaluated District procedures and examined selected backup reports to determine the adequacy of the District's data recovery procedures to restore District IT assets to a pre-incident trusted state.
- Examined network logging settings and related District reports to determine the adequacy of District logging and monitoring controls designed for the District network infrastructure supporting Skyward and Focus.
- Evaluated District procedures and examined selected District records to determine the adequacy of logging and monitoring controls over changes to critical student records and information.
- 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 records to determine the appropriateness of change management controls over Skyward and Focus.
- Examined and evaluated District procedures for managing personally owned devices connecting to the District network.
- Examined District records to evaluate the effectiveness of District security awareness training.
- 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

June 23, 2026

Ms. 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:

Thank you for the opportunity to respond to the preliminary and tentative audit findings resulting from the Information Technology Operational Audit of the Leon County District School Board's Skyward School Business Suite and Focus Student Information System. The District appreciates the professionalism and collaboration demonstrated by the Auditor General's staff throughout the audit process.

The District has reviewed the findings and recommendations and agrees with each of the findings. We are committed to maintaining strong information technology controls and continuously improving our processes to protect the confidentiality, integrity, and availability of District information systems and data.

Finding 1 – Application Security Management

District Response:
The District agrees with this finding.

The District recognizes the importance of maintaining documented evidence of periodic reviews of user access privileges to ensure that access remains appropriate and aligned with assigned job responsibilities. During the audit period, annual reviews were initiated; however, documentation and follow-up procedures were not consistently completed.

To address this finding, Technology and Information Services has established enhanced procedures requiring documented annual certification by school principals and department supervisors for all Focus and Skyward access privileges. These procedures include standardized reporting, written confirmation of access appropriateness, tracking of completion status, and retention of supporting documentation. The District will also implement escalation procedures for overdue reviews to ensure timely completion.

Anticipated Completion Date: July 2026

Finding 2 – Security Controls: User Authentication, Account Management, and Data Recovery

District Response:
The District agrees with this finding.

Because portions of this finding involve confidential cybersecurity information that is exempt from public disclosure, the District will not address specific technical details in this response. However, the District has reviewed each of the identified issues and has developed corrective action plans to address the recommendations provided by the Auditor General.

Corrective actions include enhancements to authentication controls, account management practices, privileged access management, and data recovery testing procedures. Several improvements have already been implemented, and remaining actions are currently in progress, including configuration changes, policy updates, testing, and validation activities. The District will continue to evaluate security controls against industry best practices and applicable guidance to further strengthen its cybersecurity posture.

Anticipated Completion Date: December 2026

The Leon County District School Board appreciates the Auditor General's recommendations and views this audit as an opportunity to strengthen operational and security controls. We remain committed to implementing the corrective actions described above and to maintaining effective stewardship of District information technology resources.

Sincerely,

Rocky Hanna
Superintendent
Leon County Schools