STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2026-013
August 2025

CHARLOTTE COUNTY DISTRICT SCHOOL BOARD

Focus Student Information System

Sherrill F. Norman, CPA
Auditor General

Board Members and Superintendent

During the period June 2024 through May 2025, Mark Vianello served as Superintendent of Charlotte County District School Board and the following individuals served as School Board Members:

	District No.
Cara Reynolds, Chair through 11-18-24	1
Kim Amontree	2
Robert Segur, Vice Chair from 11-19-24	3
John LeClair, Chair from 11-19-24, Vice Chair through 11-18-24	4
Wendy Atkinson	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 Drew Parker, 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

CHARLOTTE COUNTY DISTRICT SCHOOL BOARD

Focus Student Information System

SUMMARY

This operational audit of Charlotte County District School Board (District) focused on evaluating selected information technology (IT) controls applicable to the Focus Student Information System and the District's IT infrastructure and included a follow-up on the findings included in our report No. 2019-212. Our audit disclosed the following:

Finding 1: Certain District IT security controls related to user authentication, account management, data recovery, monitoring, and configuration management need improvement to ensure the confidentiality, integrity, and availability of District data and IT resources. A similar finding related to monitoring and configuration management was noted in our report No. 2019-212.

BACKGROUND

The Charlotte 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 Charlotte 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 2023-24 fiscal year, the District operated 22 elementary, middle, high, and specialized schools; sponsored 2 charter schools; and reported 20,686 unweighted full-time equivalent students.

The District uses the Focus Student Information System (Focus) to process and report student information. The software vendor, Focus School Software, Inc, hosts the Focus application and maintains and manages the supporting application and database infrastructure. The District maintains and manages the network domain supporting access to Focus and the District information technology infrastructure.

FINDING AND RECOMMENDATION

Finding 1: Security Controls – User Authentication, Account Management, Data Recovery, Monitoring, 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, monitoring, 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.

Without appropriate security controls related to user authentication, account management, data recovery, monitoring, and configuration management, 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 monitoring and configuration management was noted in our report No. 2019-212.

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

PRIOR AUDIT FOLLOW-UP

Except as discussed above, the District had taken corrective actions for the findings included in our report No. 2019-212.

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 February 2025 through May 2025 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 District IT controls applicable to Focus Student Information System (Focus) and District IT infrastructure during the period June 2024 through May 2025, and selected actions subsequent thereto. For those areas addressed by this audit, our audit objectives were to:

- Evaluate the effectiveness of selected significant 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.
- Determine whether management had taken corrective actions for the findings included in our report No. 2019-212.
- 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 Focus and IT infrastructure and to evaluate whether District operations were designed properly and operating effectively.
- Evaluated the effectiveness of District logical access controls assigned to the District network and selected network devices, including the periodic evaluation of assigned administrator access privileges.
- Evaluated the effectiveness of logical access controls for Focus, including District procedures for the periodic review of assigned user access privileges.
- 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 selected security settings related to Focus and the District network infrastructure to determine whether authentication controls were configured and enforced in accordance with IT best practices.
- 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 all accounts assigned administrator access privileges, as of February 25, 2025, within the four default network administrator system groups for the District network domain.
- Examined and evaluated the appropriateness of all accounts assigned administrator access privileges, as of February 25, 2025, for the two high risk network devices for the District network.

- 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 February 25, 2025, the 13 critical servers on the District network.
    - As of March 26, 2025, the 2 high risk network devices for the District network.
- Examined District records to evaluate 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 patches and updates and managing device end-of-life.
- Examined District records to evaluate the effectiveness of District security awareness training.
- 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 backup reports to determine the adequacy of the District data recovery procedures to restore District IT assets to a pre-incident trusted state.
- Evaluated District procedures and examined selected records to determine the appropriateness of change management controls over Focus.
- Examined network logging settings and related District reports to determine the adequacy of District logging and monitoring controls designed for the network infrastructure supporting Focus.
- 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

August 15, 2025

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

Dear Ms. Norman:

Pursuant to Section 11.45(4)(d), Florida Statutes, Charlotte County Public Schools (CCPS) submits the following written statement of explanation and corrective action in response to the preliminary and tentative audit finding provided by your Office.

Finding 1: Security Controls – User Authentication, Account Management, Data Recovery, Monitoring, and Configuration Management

Auditor Recommendation:

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

Response to Finding:

CCPS acknowledges the audit finding and is actively engaged in strengthening IT security controls in the identified areas. District staff have initiated a comprehensive review of existing practices and are implementing targeted enhancements to address identified gaps. These actions are intended to ensure that the confidentiality, integrity, and availability of District data and IT resources are maintained in alignment with recognized best practices. The District is committed to completing the planned enhancements and verifying their effectiveness through ongoing evaluation and documentation.

We appreciate the Auditor General's review and recommendations and will continue to work toward ensuring that CCPS's information technology environment remains secure, reliable, and aligned with statutory requirements.

Sincerely,

Mark Vianello
Superintendent of Schools

1445 Education Way, Port Charlotte, FL 33948 • (941) 255-0808 • fax (941) 255-7571• www.yourcharlotteschools.net