

STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2026-079
January 2026

**SANTA ROSA COUNTY DISTRICT SCHOOL
BOARD**

Focus Enterprise Resource Planning System and
Focus Student Information System



Sherrill F. Norman, CPA
Auditor General

Board Members and Superintendent

During the period October 2024 through September 2025, Dr. Karen Barber served as Superintendent of the Santa Rosa County Schools and the following individuals served as School Board Members:

	<u>District No.</u>
Linda K. Sanborn, Chair through 11-18-24	1
Elizabeth Hewey	2
Carol N. Boston, Chair from 11-19-24, Vice Chair through 11-18-24	3
Charles Elliott	4
Scott Peden, Vice Chair from 11-19-24	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 Ellen Henley, CISA, CFE, 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

SANTA ROSA COUNTY DISTRICT SCHOOL BOARD

Focus Enterprise Resource Planning System and Focus Student Information System

SUMMARY

This operational audit of Santa Rosa County School District (District) focused on selected information technology (IT) controls applicable to the Focus Enterprise Resource Planning System and Focus Student Information System (Focus) and the District's IT infrastructure. Our audit disclosed the following:

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

BACKGROUND

The Santa Rosa 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 Santa Rosa County. The governing body of the District is the Santa Rosa 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 39 elementary, middle, high, and specialized schools; sponsored 2 charter schools; and reported 31,124 unweighted full-time equivalent students.

The District uses the Focus Enterprise Resource Planning System to process and report financial and human resources information and Focus Student Information System (Focus) to process and report student information. The software vendor, Focus School Software, hosts the Focus applications and maintains and manages the supporting application and database infrastructure. In addition, the District maintains and manages the network domain and IT infrastructure supporting access to Focus.

FINDING AND RECOMMENDATION

Finding 1: Security Controls – Authentication, Account Management, Vulnerability Management, Configuration Management, Monitoring, 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 authentication, account management, vulnerability management, configuration management, monitoring, 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 seven findings in the six areas needing improvement.

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

Recommendation: We recommend that District management improve IT security controls related to authentication, account management, vulnerability management, configuration management, monitoring, and data recovery 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 information technology (IT) operational audit from June 2025 through November 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 the Focus Enterprise Resource Planning system and Focus Student Information System (Focus) and District IT infrastructure during the period October 2024 through September 2025, 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 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 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 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 Focus, including District procedures for the periodic review of assigned administrative access privileges.
- Examined and evaluated the appropriateness of all accounts assigned administrator access privileges, as of June 12, 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 June 12, 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 or port filtering 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 July 10, 2025, the 10 operating system versions installed for District devices.
 - As of June 12, 2025, the 8 critical servers and the 2 high risk network devices for the District 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.
- 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 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 District records to determine the adequacy of controls for securing data exchange between Focus and external systems.
- Evaluated District procedures and examined selected records to determine the appropriateness of change management controls over Focus.
- 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

MANAGEMENT'S RESPONSE



Dr. Karen Barber
Superintendent of Schools
6032 Highway 90
Milton, Florida 32570
Phone: 850-983-5150
Email: barberk@santarosa.k12.fl.us

January 12, 2026

Auditor General - State of Florida

Re: Management Response to Audit Finding – Security Controls

Dear Ms. Norman:

On behalf of the District, this letter transmits our formal written response to **Finding 1: Security Controls – Authentication, Account Management, Vulnerability Management, Configuration Management, Monitoring, and Data Recovery**, as identified in the recent audit.

District management acknowledges the audit finding related to the need for improvements in certain IT security controls, including authentication, account management, vulnerability management, configuration management, monitoring, and data recovery. We recognize the importance of strong and effective security controls in safeguarding the confidentiality, integrity, and availability of District data and IT resources.

District management has assigned responsibility for remediation to appropriate IT leadership and staff and is implementing corrective actions in alignment with industry best practices, applicable regulatory requirements, and District policies. Progress will be monitored, and controls will be periodically reviewed to ensure ongoing effectiveness and continuous improvement.

Management concurs with the recommendation and is committed to improving IT security controls to better protect District data and IT resources.

The District takes its responsibility to safeguard the confidentiality, integrity, and availability of data and information technology resources seriously. We appreciate the Auditor General's review and recommendations and view the audit process as an important tool for strengthening internal controls and improving operational effectiveness.

Please contact our office should additional information or clarification be required.

Respectfully submitted,

Dr. Karen Barber
Superintendent of Schools
Santa Rosa County

DISTRICT 1
Linda Sanborn

DISTRICT 2
Elizabeth Hewey

DISTRICT 3
Carol Boston

DISTRICT 4
Charles Elliott

DISTRICT 5
Scott Peden