STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2027-018
August 2026

FLORIDA SOUTHWESTERN STATE COLLEGE

Ellucian Banner
Enterprise Resource Planning System

Sherrill F. Norman, CPA
Auditor General

Board of Trustees and President

During the period May 2025 through April 2026, Dr. Jeffery S. Allbritten served as President of Florida SouthWestern State College and the following individuals served as Members of the Board of Trustees:

	County
Julia du Plooy, Chair	Hendry
David Ciccarello, Vice Chair through 8-18-25	Lee
William Banfield	Lee
Kristina Heuser J.D.	Collier
Eviana Martin J.D.	Lee
Lisa Metcalfe Swinto	Lee
Denise Murphy	Collier
Dr. Tyler Patak, Vice Chair from 8-19-25	Lee

Note: One Trustee position was vacant the entire period.

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 Shayne Alongi, 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) 412-2946.

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

FLORIDA SOUTHWESTERN STATE COLLEGE

Ellucian Banner Enterprise Resource Planning System

SUMMARY

This operational audit of Florida SouthWestern State College focused on evaluating information technology (IT) controls applicable to the Ellucian Banner Enterprise Resource Planning system (Banner) and College IT infrastructure and included a follow-up on findings included in our report No. 2020-130. Our audit disclosed the following:

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

BACKGROUND

Florida SouthWestern State College (College) is under the general direction and control of the Florida Department of Education, Division of Florida Colleges, and is governed by State law and State Board of Education rules. A Board of Trustees (Board) governs and operates the College. The Board constitutes a corporation and is composed of nine members appointed by the Governor and confirmed by the Senate. The College President serves as the Executive Officer and the Corporate Secretary of the Board and is responsible for the operation and administration of the College.

The College uses the Ellucian Banner Enterprise Resource Planning system (Banner) for recording, processing, and reporting finance, human resources, and student-related transactions. In addition, the College maintains and manages the network domain, application and database servers, and database management system supporting Banner.

FINDING AND RECOMMENDATION

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

Security controls are intended to protect the confidentiality, integrity, and availability of data and information technology (IT) resources. Our audit procedures disclosed that certain security controls related to user authentication, account management, configuration 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 College data and related IT resources. However, we have notified appropriate College management of five findings in the four areas needing improvement.

Without appropriate security controls related to user authentication, account management, configuration management, and data recovery, the risk is increased that the confidentiality, integrity, and availability of College data and related IT resources may be compromised. A similar finding related to network account management was noted in our report No. 2020-130.

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

PRIOR AUDIT FOLLOW-UP

Except as noted above, the College had taken corrective actions for the findings included in our report No. 2020-130.

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 December 2025 through June 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 College IT environment, including the critical network infrastructure supporting access to Ellucian Banner Enterprise Resource Planning System (Banner), during the period May 2025 through April 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. 2020-130.
- 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 College organizational structure and regulatory requirements, and reviewed College procedures, interviewed College personnel, and examined College records to obtain an understanding of College operations related to Banner and IT infrastructure and to evaluate whether College operations were designed properly and operating effectively.
- Evaluated selected security settings related to Banner and the College network infrastructure to determine whether authentication controls were configured and enforced in accordance with best practices.
- Evaluated the effectiveness of College logical access controls assigned to the College network, selected network devices, and IT infrastructure supporting Banner.
- Evaluated the effectiveness of logical access controls for Banner, including College procedures for the periodic evaluation of assigned user access privileges.
- Examined and evaluated the appropriateness of all accounts assigned administrator access privileges, as of December 11, 2025, within the four default network administrator system groups for the College root network domain.
- Examined and evaluated the appropriateness of all accounts assigned administrator access privileges, as of February 11, 2026, for the College's two high risk network devices.
- Evaluated College procedures and examined selected scan reports and policies to evaluate the adequacy of College vulnerability management controls related to the IT infrastructure, including vulnerability assessment and remediation, malicious software identification, and malware defense.
- Examined College records to evaluate the effectiveness of College 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 College patch management controls for operating systems and network devices to ensure that secure configurations are maintained. Specifically, we examined and evaluated:

- As of January 5, 2026, the 13 critical servers for the College network.
- As of January 27, 2026, the 3 operating system versions installed for College devices.
- As of January 29, 2026, the 2 high risk network devices for the College network.

- Examined and evaluated the appropriateness of selected administrative access privileges assigned for the 566 active accounts on the database as of January 5, 2026.
- Examined and evaluated the appropriateness of all accounts assigned access privileges, as of January 5, 2026, for the 12 application servers and the 1 database server supporting Banner.
- Examined College records supporting seven selected student records transactions and evaluated the appropriateness of user access privileges, as of January 5, 2026, granted within Banner.
- Evaluated College procedures and examined selected backup reports to determine the adequacy of the College's data recovery procedures to restore College IT assets to a pre-incident trusted state.
- Examined network logging settings and related College reports to determine the adequacy of College logging and monitoring controls designed for the College network infrastructure and database supporting Banner.
- Examined College records to determine the effectiveness of College security awareness training.
- Evaluated College procedures and examined selected records to determine the adequacy of College procedures for maintaining a software asset inventory and ensuring only authorized software is installed on the network.
- 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

FLORIDA SOUTHWESTERN STATE COLLEGE

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

Dear Ms. Norman:

Pursuant to Florida Statutes Section 11.45(4)(d), Florida SouthWestern State College is submitting to you a written response, including our proposed corrective actions to the preliminary and tentative findings of the technology operational audit dated July 21, 2026.

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

College Response:

Florida SouthWestern State College looks to continue strengthening information technology security controls related to user authentication, account management, configuration management, and data recovery.

The College takes seriously its responsibility to safeguard institutional information systems and data and has reviewed the matters communicated by the audit team. Several corrective actions identified during the audit have already been completed, with additional improvements underway. The College will continue to evaluate the effectiveness of these controls through its ongoing information security, access management, system maintenance, and disaster recovery processes.

Florida SouthWestern State College appreciates the Auditor General's review and believes the corrective actions completed and planned appropriately address the recommendation and further strengthen the confidentiality, integrity, and availability of College information systems and data.

Sincerely,

Jeffery Allbritten

President
Florida SouthWestern State College

Jason Dudley

VP Business Affairs & Technology/CIO
Florida SouthWestern State College

8099 College Parkway
Ft. Myers, FL 33919
www.FSW.edu