

STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2024-066
November 2023

NORTHWEST FLORIDA STATE COLLEGE

Ellucian Banner® Enterprise Resource Planning
System



Sherrill F. Norman, CPA
Auditor General

Board of Trustees and President

During the period March 2022 through April 2023, Dr. Devin Stephenson served as President of Northwest Florida State College and the following individuals served as Members of the Board of Trustees:

	<u>County</u>
Lori Kelley, Chair	Okaloosa
Major General (Ret.) Thomas "Rudy" Wright, Vice Chair from 7-1-22	Okaloosa
Shane Abbott, Vice Chair through 5-18-22 ^a	Walton
Charlotte Flynt	Walton
Graham Fountain	Okaloosa
Reynolds Henderson through 5-20-22 ^b	Walton
Major General (Ret.) Don Litke	Okaloosa
Jack "Tanner" Peacock from 8-5-22	Walton
Dr. Jon Ward from 8-5-22	Walton

^a Trustee position vacant from 5-19-22, through 8-4-22. Vice Chair position vacant 5-19-22, through 6-30-22.

^b Trustee position vacant from 5-21-22, through 8-4-22.

Note: One Trustee position was vacant for the entire period.

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) 412-2926.

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

NORTHWEST FLORIDA STATE COLLEGE

Ellucian Banner® Enterprise Resource Planning System

SUMMARY

This operational audit of Northwest Florida State College (College) focused on evaluating selected information technology (IT) controls applicable to the Ellucian Banner® Enterprise Resource Planning system and the College's IT infrastructure, and included a follow-up on the findings included in our report No. 2018-072. Our audit disclosed the following:

Finding 1: Certain College IT security controls related to user authentication need improvement to ensure the confidentiality, integrity, and availability of College data and IT resources. A similar finding related to user authentication was noted in our report No. 2018-072.

BACKGROUND

Northwest Florida 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 eight 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 (Banner®) system to record, process, and report finance and human resources transactions and student information. 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

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 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 the user authentication deficiencies needing improvement. A similar finding related to user authentication was noted in our report No. 2018-072.

Without appropriate security controls related to user authentication, the risk is increased that the confidentiality, integrity, and availability of College data and related IT resources may be compromised.

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

PRIOR AUDIT FOLLOW-UP

Except as discussed in Finding 1, the College had taken corrective actions for applicable components of the finding included in our report No. 2018-072.

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 2023 through September 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 College IT controls applicable to the Ellucian Banner® Enterprise Resource Planning system (Banner®) and College IT infrastructure during the period March 2022 through April 2023, 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; the safeguarding of IT resources.
- To determine whether management had corrected, or was in the process of correcting, deficiencies disclosed in our report No. 2018-072.
- 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 College organizational structure and regulatory requirements; 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 the sufficiency of College controls, observed, documented, and tested key processes, procedures, and controls related to Banner® and College IT infrastructure, including authentication, backup and recovery, configuration of systems, logical controls, and inventory and vulnerability management.
- Examined selected security settings related to College network infrastructure, Banner® and database, 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 College logical access controls assigned to the College network, selected network devices, database, and servers supporting Banner®, including the periodic evaluation of assigned accounts.
- Examined and evaluated the appropriateness of all accounts assigned administrator access privileges, as of February 15, 2023, within the four default network administrator system groups for the College root domain.
- Examined and evaluated, as of February 15, 2023, the nine root domain user accounts not required to have a password change.
- Examined and evaluated the appropriateness of all accounts assigned administrator access privileges, as of March 7, 2023, for the two College high-risk network devices.
- Examined and evaluated the appropriateness of all services enabled on 3 of the 15 servers supporting Banner®. Specifically, we examined and evaluated:
 - All services on the database server as of June 19, 2023.
 - All services on the two select application servers hosting Banner® self-service as of July 31, 2023.
- Examined and evaluated the appropriateness of access privileges granted on the 3 portal servers for the 25 user and high-risk accounts as of February 16, 2023.

- Examined and evaluated the appropriateness of access privileges granted on the portal administration server for the nine user and high-risk accounts as of February 17, 2023.
- Examined and evaluated the appropriateness of access privileges granted on the portal authentication server for the seven user and high-risk accounts as of February 16, 2023.
- Examined and evaluated the appropriateness of access privileges granted on 3 of the 15 servers supporting Banner®. Specifically, we examined:
 - The 12 user and high-risk accounts assigned, as of February 15, 2023, to 1 of the 2 selected application servers hosting Banner self-service.
 - The 11 user and high-risk accounts assigned, as of February 16, 2023, to the second select application server hosting Banner self-service.
 - The 9 user and high-risk accounts assigned, as of February 17, 2023, to the database server.
- Examined and evaluated the appropriateness of the 38 accounts assigned selected administrative access privileges, as of February 2, 2023, to the database supporting Banner®.
- Examined and evaluated selected College patch management controls for operating systems and network devices to ensure secure configurations are maintained. Specifically, we examined and evaluated:
 - The 59 network servers as of July 12, 2023.
 - The 15 Banner® servers as of June 19, 2023.
 - The two high-risk network devices as of March 7, 2023.
- Evaluated College procedures and examined selected backup and testing reports to determine the adequacy of the College data recovery procedures to restore College IT assets to a pre-incident trusted state.
- Evaluated the effectiveness of College 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 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.
- Evaluated the effectiveness of College security awareness training.
- Evaluated College procedures and examined selected scan reports 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.
- Evaluated College procedures and reviewed reports related to the recording, documenting, and reporting of changes to confidential and critical student record information within the Banner® ERP system student module to determine the adequacy of College logging and monitoring controls related to student information.
- Examined selected database and server security and error logs to determine the adequacy of College logging and monitoring controls designed for the infrastructure supporting Banner®, including actions performed by privileged users.
- 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 finding and recommendation included in this report and which describes 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



NORTHWEST FLORIDA STATE COLLEGE

100 College Boulevard, E. • Niceville, FL 32578-1347 • (850) 678-5111 • www.nwfsc.edu

November 15, 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,

I am writing to address the preliminary and tentative audit finding and recommendation arising from the Information Technology operational audit of Northwest Florida State College, Ellucian Banner® Enterprise Resource Planning system.

In accordance with Section 11.45(4)(d) of the Florida Statutes, we present this written statement providing clarification on the identified finding, encompassing both our current and planned corrective measures. The subsequent section outlines our response to the identified issue.

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

Response: Northwest Florida State College is actively expanding the use of multi-factor authentication to meet the standards identified by the auditor staff.

Sincerely,

A handwritten signature in black ink, appearing to read "Cole Allen", with a long horizontal line extending to the right.

Cole Allen
AVP, Information Technology & CIO

NWF State College Fort Walton Beach Campus • (850) 863-6500
Chautauqua Center, DeFuniak Springs • (850) 200-4100 Hurlburt Center, Hurlburt Field • (850) 200-4190
Robert L. F. Sikes Education Center, Crestview • (850) 200-4141 South Walton Center, Santa Rosa Beach • (850) 200-4160
An Equal Access/Equal Opportunity Institution