STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2025-005
July 2024

UNIVERSITY OF WEST FLORIDA

Ellucian Banner® Enterprise Resource Planning System

Sherrill F. Norman, CPA
Auditor General

Board of Trustees and President

During the period, April 2023 through March 2024, Dr. Martha Saunders served as President of the University of West Florida and the following individuals served as Members of the Board of Trustees:

Suzanne Lewis, Chair
Jill Singer, Vice Chair
Richard R. Baker
Dr. Paul Hsu
Dr. Susan James from 8-1-23 [a]
Patrick Marshall through 4-6-23 [b]
Ariauna Range from 4-7-23 [b]
Dr. Sherry Schneider through 7-31-23 [a]
Alonzie Scott
Robert D. Sires through 2-20-24 [c]
Stephanie White

[a] Faculty Senate President.
[b] Student Body President.
[c] Trustee position vacant from 2-21-24 through 3-31-24.
[d] Four Trustee positions vacant during the audit period.

The team leader was Joseph Clayton 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

UNIVERSITY OF WEST FLORIDA

Ellucian Banner® Enterprise Resource Planning System

SUMMARY

This operational audit of University of West Florida (University) focused on selected information technology (IT) controls applicable to the Ellucian Banner® Enterprise Resource Planning system (Banner®) and the University's IT infrastructure, and included a follow-up on findings noted in our report No. 2019-007. Our audit disclosed the following:

Finding 1: University IT security controls related to information security, authentication, account management, vulnerability management, data recovery, and monitoring need improvement to ensure the confidentiality, integrity, and availability of University data and IT resources. A similar finding related to information security and monitoring was noted in our report No. 2019-007.

BACKGROUND

The University of West Florida (University) is part of the State university system of public universities, which is under the general direction and control of the Florida Board of Governors (BOG). The University is directly governed by a Board of Trustees (Trustees) consisting of 13 members. The Governor appoints 6 citizen members and the BOG appoints 5 citizen members. These members are confirmed by the Florida Senate and serve staggered 5-year terms. The Faculty Senate Chair and Student Body President are also members. The BOG establishes the powers and duties of the Trustees. The Trustees are responsible for setting University policies, which provide governance in accordance with State law and BOG Regulations. The University President is selected by the Trustees and confirmed by the BOG. The University President serves as the Executive Officer and the Corporate Secretary of the Trustees and is responsible for administering the policies prescribed by the Trustees for the University.

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

FINDING AND RECOMMENDATION

Finding 1: Security Controls – Information Security, Authentication, Account Management, Vulnerability Management, Data Recovery, and Monitoring

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed certain security controls related to information security, authentication, account management, vulnerability management, data recovery, and monitoring need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising the confidentiality of University data and related IT resources. However, we have notified

appropriate University management of the seven findings in the six areas needing improvement. A similar finding related to information security and monitoring was noted in our report No. 2019-007.

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

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

PRIOR AUDIT FOLLOW-UP

Except as discussed in Finding 1, the University had taken corrective actions for the findings included in our report No. 2019-007.

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 January 2024 through June 2024 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 IT controls applicable to the Ellucian Banner® Enterprise Resource Planning system (Banner®) and University IT infrastructure during the period April 2023 through March 2024, 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 taken corrective actions for findings included in our report No. 2019-007.
- 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 University organizational structure and regulatory requirements; reviewed University procedures, interviewed University personnel, and examined University records to obtain an understanding of University operations related to Banner® and IT infrastructure and to evaluate whether University operations were designed properly and operating effectively.
- Evaluated the sufficiency of University controls and observed, documented, and tested key processes, procedures, and controls related to Banner® and University IT infrastructure, including authentication, backup and recovery, configuration of systems, logical controls, logging and monitoring, and inventory and vulnerability management.
- Examined selected security settings related to University network infrastructure, externally facing applications, 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 University logical access controls assigned to the University network, selected network devices, database, authentication server, Banner® application and database servers, and the Banner® student module, including the periodic evaluation of assigned accounts.
- Examined seven selected student records transactions and evaluated the appropriateness of user access privileges, as of January 17, 2024, granted within the Banner® ERP system.
- Evaluated the University's information security program, including the University risk assessment.
- Examined and evaluated the appropriateness of all accounts assigned administrator access privileges, as of January 12, 2024, within the four default network administrator system groups for the University root domain.

- Examined and evaluated the appropriateness of all accounts assigned administrator access privileges, as of January 12, 2024, for the two University high risk network devices for the root domain.
- Examined and evaluated the appropriateness of all accounts assigned selected administrative access privileges to the authentication server and four servers supporting Banner®. Specifically, we examined and evaluated:
    - The 42 accounts on the authentication server as of May 29, 2024.
    - The 31 accounts assigned on the three Banner® application servers and 57 accounts assigned on the Banner® database server as of March 1, 2024.
- Examined and evaluated selected University patch management controls for operating systems and network devices to ensure secure configurations are maintained. Specifically, we examined and evaluated:
    - As of March 1, 2024, the six critical network servers and the two high-risk network devices for the root domain.
    - As of April 4, 2024, the three Banner® application servers and one database server.
- Examined and evaluated the appropriateness of the 26 user accounts granted database administration privileges as of January 17, 2024.
- Examined and evaluated the appropriateness of selected administrative access privileges as of January 17, 2024, for the 36 active accounts granted direct login capability for the database. Evaluated University procedures and examined selected database logs to determine the adequacy of University logging and monitoring controls designed for the Banner® database, including actions performed by privileged users.
- Evaluated University procedures and examined selected backup and testing reports to determine the adequacy of the University data recovery procedures to restore University IT assets to a pre-incident trusted state.
- Evaluated the effectiveness of University 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 University procedures and examined selected records to determine the adequacy of University procedures for maintaining a software asset inventory and ensuring only authorized software is installed on the network.
- Evaluated the effectiveness of University security awareness training.
- Evaluated University procedures and examined selected scan reports and policies to evaluate the adequacy of University vulnerability management controls related to the IT infrastructure, including vulnerability assessment and remediation, penetration testing, malicious software identification, and malware defense.
- 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

Office of the President
11000 University Parkway
Pensacola, FL 32514

July 17, 2024

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

Subject: Response to Preliminary & Tentative Audit Finding

Dear Ms. Norman,

This is our response to the preliminary and tentative audit finding and recommendation included in your recent communication regarding the information technology operational audit of the University of West Florida, Ellucian Banner® Enterprise Resource Planning System.

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

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

Management Response: We have reviewed the items detailed in the report and initiated an internal project to assess and address the identified deficiencies in our current IT security measures. We will develop individual action plans for each area highlighted in the audit. Our corrective actions will include:

- Enhancing information security protocols and policies;
- Improving authentication processes;
- Implementing more strict account management procedures;
- Advancing vulnerability management strategies;
- Strengthening data recovery plans; and
- Upgrading monitoring systems.

office 850.474.2200
fax 850.474.3131
uwf.edu

We appreciate the audit team's efforts in identifying these critical areas for improvement and are committed to addressing these issues promptly and effectively.

Sincerely yours,

Martha D. Saunders, Ph.D.
President

cc: Jaromy Kuhl, Provost
Geissler Golding, CIO and CISO
Cindy Talbert, Chief Audit Executive