

Report No. 2024-195
April 2024

STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

EASTERN FLORIDA STATE COLLEGE

Ellucian Banner® Enterprise Resource Planning
System



Sherrill F. Norman, CPA
Auditor General

Board of Trustees and President

During the period September 2022 through October 2023, Dr. James H. Richey served as President of Eastern Florida State College and the following individuals served as Members of the Board of Trustees:

Ronald S. Howse, Chair
Dr. Edgar Figueroa, Vice Chair
Bruce Deardoff
Laura Moody
Winston Scott

The team leader was George W. Phillips, CISSP, 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

EASTERN FLORIDA STATE COLLEGE

Ellucian Banner® Enterprise Resource Planning System

SUMMARY

This operational audit of Eastern Florida State College (College) focused on 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 finding noted in our report No. 2018-203. Our audit disclosed the following:

Finding 1: Certain College IT security controls related to authentication, account management, configuration management, logging and monitoring, and vulnerability management need improvement to ensure the confidentiality, integrity, and availability of College data and IT resources. A similar finding related to authentication and logging and monitoring was noted in our report No. 2018-203.

BACKGROUND

Eastern 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 five 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®) 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 - Authentication, Account Management, Configuration Management, Logging and Monitoring, and Vulnerability 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 authentication, account management, configuration management, logging and monitoring, and vulnerability management 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 five findings in the areas needing improvement. A similar finding related to authentication and logging and monitoring was noted in our report No. 2018-203.

Without appropriate security controls related to authentication, account management, configuration management, logging and monitoring, and vulnerability management, 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 authentication, account management, configuration management, logging and monitoring, and vulnerability management 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. 2018-203.

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 August 2023 through February 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 College IT controls applicable to the Ellucian Banner® Enterprise Resource Planning system (Banner®) and College IT infrastructure during the period September 2022 through October 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; and the safeguarding of IT resources.
- To determine whether management had taken corrective actions for the finding included in our report No. 2018-203.
- 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 and 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, logging and monitoring, and inventory and vulnerability management.
- Examined selected security settings related to College 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 College logical access controls assigned to the College network, selected network devices, database and server, 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 August 10, 2023, within the four default network administrator system groups for the College forest domain containing staff accounts.
- Examined and evaluated, as of August 10, 2023, the password change interval of the 636 accounts assigned across the 12 critical servers supporting Banner®.
- Examined and evaluated the appropriateness of all accounts assigned administrator access privileges, as of September 18, 2023, for the two College high-risk network devices for the staff forest domain.

- Examined and evaluated the appropriateness of all accounts assigned selected administrative access privileges, as of August 10, 2023, to the 12 critical servers 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:
 - As of September 18, 2023, the 12 critical network servers, the 12 critical servers supporting Banner®, and the 2 database servers.
 - As of September 27, 2023, the 2 high-risk network devices for the staff forest domain.
- Examined and evaluated the appropriateness of all services enabled on the production database server as of August 10, 2023.
- Examined and evaluated the appropriateness of the four user accounts granted direct login capability for the database as of August 10, 2023.
- Examined and evaluated the appropriateness of the 26 accounts assigned on the production database server as of August 10, 2023.
- Examined and evaluated the appropriateness of selected administrative access privileges assigned for the 216 active accounts on the database as of August 10, 2023.
- Evaluated College procedures and examined selected database and server security logs to determine the adequacy of College logging and monitoring controls designed for the infrastructure supporting Banner®, including actions performed by privileged users.
- 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 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.
- 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.

A handwritten signature in blue ink that reads "Sherrill F. Norman". The signature is fluid and cursive, with the first name being the most prominent.

Sherrill F. Norman, CPA
Auditor General

MANAGEMENT'S RESPONSE



President

James H. Richey, J.D.

Board of Trustees

Ronald Howse, Chair
Dr. Edgar Figueroa, Vice Chair
R. Bruce Deardoff
Laura Moody
Winston Scott

Cocoa Campus

1519 Clearlake Road
Cocoa, Florida 32922
321/632-1111
Fax: 321/433-7064

Melbourne Campus

3865 N. Wickham Road
Melbourne, Florida 32935
321/632-1111
Fax: 321/433-5618

Palm Bay Campus

250 Community College Pkwy.
Palm Bay, Florida 32909
321/632-1111
Fax: 321/433-5305

Titusville Campus

1311 North U.S. 1
Titusville, Florida 32796
321/632-1111
Fax: 321/433-5113

easternflorida.edu



April 9, 2024

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

RE: EFSC Information Technology Operational Audit Response

Dear Ms. Norman:

The following is the response to the preliminary and tentative finding of your information technology operational audit of the Eastern Florida State College, Ellucian Banner® Enterprise Resource Planning System.

Finding 1: Security Controls - Authentication, Account Management, Configuration Management, Logging and Monitoring, and Vulnerability Management

The College agrees with the findings and recommendation included in the report. We have taken appropriate corrective actions to improve security controls related to authentication, account management, configuration management, logging and monitoring, and vulnerability management to ensure the confidentiality, integrity, and availability of College data and IT resources.

Sincerely,

A handwritten signature in blue ink that reads "James H. Richey".

Dr. James H. Richey, President
Eastern Florida State College

JHR/mm