STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2022-007
August 2021

ST. JOHNS RIVER STATE COLLEGE

Ellucian Banner®
Enterprise Resource Planning System

Sherrill F. Norman, CPA
Auditor General

Board of Trustees and President

During the period November 2019 through December 2020, Mr. Joe H. Pickens, J.D. served as President of St. Johns River State College, and the following individuals served as Members of the Board of Trustees:

	County
Samuel Garrison, Chair	Clay
Wendell D. Davis, Vice Chair	Clay
Robert Crum	St. Johns
Jan Conrad	St. Johns
Leslie Dougher through 12-22-20	Clay
Brian Keith	Putnam
James E. Reid	Putnam
W.J. (Jud) Sapp Jr. from 12-23-20	Clay

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

ST. JOHNS RIVER STATE COLLEGE

Ellucian Banner® Enterprise Resource Planning System

SUMMARY

This operational audit of St. Johns River State College (College) focused on evaluating selected information technology (IT) controls applicable to the Ellucian Banner® Enterprise Resource Planning (Banner® ERP) system for maintaining and processing student account information, the College's compliance with the Federal Trade Commission Standards for Safeguarding Customer Information (Safeguards Rule), and the infrastructure supporting the College Banner® ERP system. Our audit disclosed the following:

Finding 1: College controls over application security management need improvement to ensure that access privileges to student information granted within the Banner® ERP system are necessary and appropriate.

Finding 2: College IT security controls over user authentication, monitoring, and account management need improvement to ensure the confidentiality, integrity, and availability of College data and IT resources.

BACKGROUND

St. Johns River 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 seven 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® ERP) system to record, process, and report finance and human resources transactions and student information. As an institution of higher learning, the College is defined as a financial institution by the Federal Trade Commission and, therefore, is subject to the provisions of the Gramm-Leach-Bliley Act. In addition, the College maintains and manages the network domain, Web, application, and database servers, and database management system supporting the Banner® ERP system.

FINDINGS AND RECOMMENDATIONS

Finding 1: Application Security Management

Access controls are intended to protect data and information technology (IT) resources from unauthorized disclosure, modification, or destruction. Effective access controls include granting employees access to IT resources based on a demonstrated need to view, change, or delete data and restricting employees from performing incompatible functions or functions outside of their areas of responsibility.

Security within the Banner® ERP system student module is based on controlling users' access to forms that relate to functions necessary for student administration, curriculum management, and student record maintenance. Through inquiry with College personnel and examination of College records, we identified eight forms that allowed access to view or modify critical or confidential student related information, including course information and student academic history, residency status, demographic and personally identifiable information (name, personal identifier, date of birth), placement test scores, and other course, graduation, and transfer data.

Our examination of the access privileges as of October 2020 for all 172 Banner® ERP system user accounts assigned one or more of the eight forms disclosed that access privileges were not always restricted to employee-assigned responsibilities. Specifically:

- Because College management focused on the ability to modify critical data within the Banner® ERP system in assigning access privileges, 36 employees throughout the College had the ability to view all students' protected student record information, including personally identifiable information, academic history, and placement test scores.
- 3 human resources employees had the ability to modify student record information and 2 of the 3 employees had the ability to update personally identifiable information. The other employee had the ability to modify student residency status, academic history, placement test scores, personally identifiable information, and College course data. The ability to modify student record and course information was not necessary for any of these 3 employees' job responsibilities.
- Although unnecessary for her assigned job responsibilities, a secretary had the ability to modify placement test scores.
- 3 IT staff had the ability to modify students' academic history and transfer data. In response to our inquiry, College management indicated that IT staff may assist the users in troubleshooting issues within the application. Notwithstanding the need for IT staff to facilitate processing support for the end users, the IT employees' daily responsibilities did not require update access privileges to student information within the Banner® ERP system.

In response to our inquiry, College management indicated that some of the access privileges noted had been removed and that, going forward, critical forms would be reassessed for granting view access privileges based on the confidential nature of the information. Appropriately restricted access privileges help protect College data and IT resources from unauthorized modification, loss, and disclosure.

Recommendation: College management should ensure that the access privileges granted to student information within the Banner® ERP system are necessary and appropriate for the employee's assigned responsibilities.

Finding 2: Security Controls – User Authentication, Monitoring, Account 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 over user authentication, monitoring, and account 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 specific issues.

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

Recommendation: College management should improve IT security controls related to user authentication, monitoring, and account management to ensure the confidentiality, integrity, and availability of College 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 IT operational audit from September 2020 through May 2021 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 College IT controls applicable to the Ellucian Banner® Enterprise Resource Planning (Banner® ERP) system for maintaining and processing student account information, the College's compliance with Safeguards Rule, and the Banner® ERP system supporting infrastructure during the period November 2019 through December 2020, and selected actions subsequent thereto. For those areas addressed by this audit, our audit objectives were:

- To determine the effectiveness of selected IT controls in achieving management's control 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, abuse, or inefficiency.

In conducting this audit, we:

- Reviewed applicable laws, rules, Board policies, College procedures, and other guidelines, interviewed College personnel, and examined College records to obtain an understanding of College operations related to the Banner® ERP system 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 the College's IT processes for the Banner® ERP system infrastructure, including authentication, logical controls, vulnerability management, logging and monitoring of the network, Web, application, and database servers (servers), and the database management system (database); Banner® ERP system application change management; and the information security program addressing student records and information, including the program coordinator designation.
- Evaluated the effectiveness of College logical access controls assigned to the College network, servers, and database supporting the Banner® ERP system, including the periodic evaluations of assigned accounts.
- Evaluated the effectiveness of logical controls assigned within the Banner® ERP system student module, including College procedures related to the periodic evaluation of assigned user access privileges.
- Examined and evaluated the appropriateness of all accounts assigned administrator access privileges within the four default network administrator system groups for the College root domain as of October 14, 2020.
- Examined and evaluated the 201 domain accounts not required to have a password change as of October 14, 2020.
- Examined and evaluated the appropriateness of access privileges granted on the 14 servers supporting the Banner® ERP system. Specifically, as of October 22, 2020, we examined:
    - The 46 accounts assigned on the database server supporting the Banner® ERP system.
    - The 47 accounts assigned to one application server and the 47 accounts assigned to the additional application server.
    - The 50 accounts assigned to the authentication server.
    - All accounts assigned to the ten Web servers. Specifically:
        - The 49 accounts assigned to each of 2 servers.
        - The 48 accounts assigned to each of 2 servers.

    - The 47 accounts assigned to each of 5 servers.
    - The 38 accounts assigned to 1 server.
- Examined and evaluated the appropriateness of the 16 accounts assigned selected administrative access privileges, as of October 14, 2020, to the database supporting the Banner® ERP system.
- Evaluated selected security settings related to the Banner® ERP system and the supporting infrastructure to determine whether authentication controls were configured and enforced in accordance with IT best practices.
- Examined and evaluated the appropriateness of access privileges, as of October 14, 2020, granted within the Banner® ERP system student module for the 172 accounts with access to one or more of the eight forms granting access to confidential or critical student record fields.
- Evaluated College procedures related to Banner® ERP system patches, upgrades, and data fixes and changes to supporting infrastructure, including system software and selected firewalls to determine whether modifications required appropriate authorization, testing, and approval.
- Examined selected database and server logs to determine the adequacy of College logging and monitoring controls designed for the infrastructure supporting the Banner® ERP system, including actions performed by privileged users.
- 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 scan reports, audit policies, logs, alert messages, and documents to evaluate the adequacy of the College vulnerability management controls related to the IT infrastructure supporting the Banner® ERP system, including secure configurations, vulnerability assessment and remediation, maintenance, monitoring, and analysis of audit logs, and malware defense.
- Evaluated selected documents and records related to the College information security program to determine compliance with the Safeguards Rule.
- 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

ST. JOHNS RIVER STATE COLLEGE

JOE H. PICKENS, J.D., PRESIDENT
5001 ST. JOHNS AVENUE | PALATKA, FL 32177-3807
(386) 312-4113 | JoePickens@SJRstate.edu

PALATKA CAMPUS 5001 ST. JOHNS AVENUE
PALATKA, FL 32177-3807 | (386) 312-4200

ST. AUGUSTINE CAMPUS 2990 COLLEGE DRIVE
ST. AUGUSTINE, FL 32084-1197 | (904) 808-7400

ORANGE PARK CAMPUS 283 COLLEGE DRIVE
ORANGE PARK, FL 32065-7639 | (904) 276-6800

SJRstate.edu
EQUAL OPPORTUNITY/EQUAL ACCESS COLLEGE

July 29, 2021

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

Dear Ms. Norman:

Pursuant to Section 11.45(4)(d), Florida Statutes, St. Johns River State College is submitting you a written statement of explanation concerning all the findings, including our actual or proposed corrective actions to the preliminary and tentative findings of the Information Technology Operational audit of the St. Johns River State College, Ellucian Banner® Enterprise Resource Planning System dated July 22, 2021.

Finding 1: Application Security Management
College Response: SJR State will redefine and resecure all critical forms and enhance the security review process.

Finding 2: Security Controls – User Authentication. Monitoring, Account Management
College Response: SJR State made changes to address user authentication and account management during the audit. We have implemented measures related to additional account management controls and monitoring to ensure the confidentiality, integrity, and availability of college data and related IT resources.

Sincerely,

Joe H. Pickens, J.D.
President
St. Johns River State College

cc: Dr. Ros Humerick
Dr. Lynn Powers
Randy Peterson
Richard Anderson