

**LAKE-SUMTER STATE COLLEGE**

Ellucian Banner® Enterprise Resource Planning  
System



Sherrill F. Norman, CPA  
Auditor General

## Board of Trustees and President

During the period, April 2020 through April 2021, Dr. Stanley M. Sidor served as President of Lake-Sumter State College and the following individuals served as Members of the Board of Trustees:

	<u>County</u>
Peter F. Wahl, Chair	Sumter
Emily A. Lee, Vice Chair	Lake
Bryn Blaise	Sumter
Marcia M. Butler	Sumter
David Hidalgo	Lake
Jennifer S. Hill	Lake
Jennifer Hooten	Sumter
Bret D. Jones	Lake
Timothy Morris	Lake

The team leader was Joseph D. Garcia, CISA, 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](mailto: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](http://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**

# LAKE-SUMTER STATE COLLEGE

## Ellucian Banner® Enterprise Resource Planning System

### **SUMMARY**

---

This operational audit of Lake-Sumter State College (College) focused on evaluating selected information technology (IT) controls applicable to Ellucian Banner® Enterprise Resource Planning (Banner® ERP) system for maintaining and processing student account information and the infrastructure supporting the College Banner® ERP system. Our operational 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 related to user authentication, account management, monitoring, and vulnerability management need improvement to ensure the confidentiality, integrity, and availability of College data and IT resources.

### **BACKGROUND**

---

Lake-Sumter 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 (Banner® ERP) 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 the Banner® ERP system.

### **FINDINGS AND RECOMMENDATIONS**

---

#### **Finding 1: Application Security Management**

Effective application security management controls include resource owners identifying specific employees and authorizing the nature and extent to which those employees may access the resources where the owner has functional responsibility. Granting access to information technology (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 is necessary to protect data and IT resources from unauthorized disclosure, modification, or destruction. In addition, documented periodic evaluations of access privileges associated with security groups help ensure that access privileges provided to each security group remain appropriate and necessary.

Banner® ERP system forms are screens or pages that allow either data field modification, view, or both. 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. However, as of April 2021, College personnel indicated that the College had not established procedures that required periodic evaluations of access privileges granted to critical forms within the Banner® ERP system student module to ensure the privileges were appropriate and necessary.

Examination of College records and responses to our inquiries disclosed that 12 forms allowed access to view or modify critical or confidential student related information, including course information and student academic history, demographic and personally identifiable information (name, personal identifier, date of birth), placement test scores, and other admissions, graduation, and transfer data. Two of the forms examined specifically allow a student's residency status to be updated by users with access to the form. Pursuant to State law,<sup>1</sup> students must be classified as residents or nonresidents for the purposes of assessing tuition in postsecondary education programs offered in Florida College System institutions.

Our examination of the access privileges as of February 2021 for all 76 active Banner® ERP system accounts assigned one or more of the 12 forms disclosed that:

- 18 employees could update course information, demographic and personally identifiable information, placement test scores, and other admissions, graduation, and transfer data,<sup>2</sup> although such updates were not part of their assigned duties. In addition, 13 of the 18 employees and 21 other employees were granted access privileges to one or both of the forms that allowed inappropriate or unnecessary update access privileges to student residency status.<sup>3</sup>

Subsequent to our inquiry, College management indicated that, as of December 2021, the inappropriate access privileges assigned to one or more of the forms evaluated for the 39 employees had been removed or changed to inquiry.

- 10 of the 76 employees<sup>4</sup> had access to appropriate data fields within one or both of the residency forms to update student registration and program information, academic standing, and campus location for advising. Although the 10 employees did not have responsibilities for assessing tuition, because the update access privileges were granted to all other data fields within the forms, they had the ability to update student residency status and impact student tuition assessments.

As of December 2021, the 10 employees continued to have the inappropriate access to update student residency status and impact student tuition assessments because the College had not determined how to modify that access.

Appropriately restricted access privileges help protect College data and IT resources from unauthorized modification, loss, or disclosure.

**Recommendation: College management should enhance procedures to ensure that the access privileges granted to student information within the Banner® ERP system are necessary and**

---

<sup>1</sup> Section 1009.21, Florida Statutes.

<sup>2</sup> Employees with inappropriate or unnecessary access privileges included, for example, a Payroll Manager who did not require the ability to update student test information; an administrative assistant who did not require the ability to perform registration overrides; and the Executive Director of Facilities who did not require the level of access granted based on the position responsibilities.

<sup>3</sup> Employees with inappropriate or unnecessary access privileges included, for example, a Data Analyst, the Dean of Students, and an Assistant Director for Student Life who did not require the ability to update student residency status and the Executive Director for Athletics who only needed to view one of the forms that included student residency status.

<sup>4</sup> The 10 employees included 2 of the 13 employees who had inappropriate update access to student residency status.

appropriate for the employee's assigned responsibilities and are periodically evaluated. Procedural enhancements should include appropriate access modifications to ensure that employees responsible for updating student registration and program information, academic standing, and campus location for advising do not have the ability to update student residency status and tuition assessments.

## **Finding 2: Security Controls – User Authentication, Account Management, 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 over user authentication, account management, 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 specific issues.

Without appropriate security controls related to user authentication, account management, 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:** College management should improve IT security controls related to user authentication, account management, monitoring, and vulnerability 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 information technology (IT) operational audit from December 2020 through December 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 significant College IT controls applicable to the Ellucian Banner® Enterprise Resource Planning (Banner® ERP) system for maintaining and processing student account information and the Banner® ERP system supporting infrastructure during the period April 2020 through April 2021, and selected actions subsequent thereto. For those areas addressed by this audit, our audit objectives were:

- To evaluate the effectiveness of selected significant 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, College policies and 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, application and database servers (servers), and the database management system (database); and Banner® ERP system application, supporting server, database, and network device change management.
- 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, as of December 11, 2020, the 190 root domain accounts not required to have a password change.

- Examined selected procedures, reports, and documents to evaluate the adequacy of College vulnerability management controls related to the IT infrastructure supporting the Banner® ERP system, including secure configurations, vulnerability assessment and remediation, maintenance, monitoring, and malware defense.
- Evaluated College procedures related to Banner® ERP system patches, upgrades, and changes to supporting infrastructure, including system software and selected firewalls to determine whether modifications required appropriate authorization, testing, and approval.
- Evaluated the effectiveness of College logical access controls assigned to the College network, servers, and database supporting the Banner® ERP system, including periodic evaluations of assigned accounts.
- Examined and evaluated the appropriateness of all accounts assigned administrator access privileges, as of December 10, 2020, within the four default network administrator system groups for the College root domain and three of the four Windows application servers and the database server supporting the Banner® ERP system.
- Examined and evaluated the appropriateness of the 36 accounts assigned selected administrative access privileges, as of February 3, 2021, to the database supporting the Banner® ERP system.
- Examined and evaluated, as of February 3, 2021, the appropriateness of the 24 accounts with default passwords defined to the database supporting the Banner® ERP system.
- Examined and evaluated, as of January 28, 2021, all privileged accounts defined to the database supporting the Banner® ERP system not required to have a password change.
- 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 access privileges, as of February 3, 2021, granted within the Banner® ERP system student module for the 76 accounts with access to one or more of the 12 forms granting access to confidential or critical student record fields.
- Examined selected network settings and database 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 related to the recording, documentation, 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.
- 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 written in a cursive style with a large initial "S".

Sherrill F. Norman, CPA  
Auditor General

## MANAGEMENT'S RESPONSE

---



February 28, 2022

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

Dear Ms. Norman,

The attached is Lake-Sumter State College's response to the preliminary and tentative findings and recommendations pertaining to the 2021 Information Technology Operational Audit.

Should you have any questions on any of our responses please don't hesitate to contact me at 353-365-3525.

Sincerely,

DocuSigned by:

*Dr. Heather Bigard*

BC2472B0495E4E6...  
Dr. Heather Bigard

Acting President

Provost & Executive Vice President

Lake-Sumter State College

L E E S B U R G • S U M T E R • S O U T H L A K E

9501 U.S. HIGHWAY 441 • LEESBURG, FLORIDA • 34788-3950 • P: 352.787.3747 • W: LSSC.EDU

Lake-Sumter State College

Responses to preliminary and tentative findings and recommendations pertaining to the 2021  
Information Technology Operational Audit  
Conducted by the Auditor General's Office

**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.

**Recommendation:** College management should enhance procedures to ensure that the access privileges granted to student information within the Banner® ERP system are necessary and appropriate for the employee's assigned responsibilities and are periodically evaluated. Procedural enhancements should include appropriate access modifications to ensure that employees responsible for updating student registration and program information, academic standing, and campus location for advising do not have the ability to update student residency status and tuition assessments.

**Management's Response:** The College agrees with the recommendations and will enhance procedures to ensure that access granted to student information within the Banner ERP system is necessary and appropriate for the business of supporting our students. We have improved the quality of the Banner and Oracle database security reports that are available to the functional staff. This will allow those responsible within each functional area to perform periodic comprehensive evaluations of staff's security access in Banner and the Oracle database. These reviews will be performed semi-annually.

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

**Recommendation:** College management should improve IT security controls related to user authentication, account management, monitoring, and vulnerability management to ensure the confidentiality, integrity, and availability of College data and IT resources.

**Management's Response:** The College has reviewed the findings and will continue to evaluate and implement improvements to the IT security controls related to user authentication, account management, monitoring and vulnerability management to ensure the confidentiality, integrity, and availability of College data and IT resources.