

STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2021-033
October 2020

STATE COLLEGE OF FLORIDA, MANATEE-SARASOTA

Ellucian Banner®
Enterprise Resource Planning System



Sherrill F. Norman, CPA
Auditor General

Board of Trustees and President

During the period March 2019 through December 2019, Dr. Carol Probstfeld served as President of the State College of Florida, Manatee-Sarasota, and the following individuals served as Members of the Board of Trustees:

	<u>County</u>
Robert A. Wyatt, Chair	Sarasota
Edward A. Baily, Vice-Chair	Manatee
Jaymie Carter	Manatee
Dominic DiMaio	Manatee
Richard Dorfman	Sarasota
John Home	Manatee
Tracy Knight	Sarasota
Rod P. Thomson	Sarasota

Note: One Board Member position was vacant during the period.

The team leader was Vikki Mathews, 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 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

STATE COLLEGE OF FLORIDA, MANATEE-SARASOTA

Ellucian Banner® Enterprise Resource Planning System

SUMMARY

This operational audit of State College of Florida, Manatee-Sarasota (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's Banner® ERP system. Our audit disclosed the following:

Finding 1: Some College employees' access privileges granted within the Banner® ERP system were contrary to an appropriate separation of end-user and technical support functions.

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

BACKGROUND

State College of Florida, Manatee-Sarasota (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 9 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, application and database servers, and database management system supporting the Banner® ERP system.

FINDINGS AND RECOMMENDATIONS

Finding 1: Access Privileges

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

The Banner® ERP system forms are screens or pages that allow either data field modification, view, or both. Security is based on controlling a user's access to these forms. Forms within the student module of the Banner® ERP system relate to functions necessary for student administration, including curriculum management, admissions, registration, scheduling, academic history, and student record information (e.g., biographical, personally identifiable, and residency status information).

As part of our audit procedures, we identified 11 forms that allowed access to update critical or confidential data. Student-related information that could be modified through these forms included restrictions for class registration, charges and financial aid awards, residency status for tuition cost determination, final grades, courses repeated, degrees conferred, and demographic information for new and existing students. Our examination of the access privileges for all 78 Banner users assigned 1 or more of the 11 forms indicated that the Information Technology Services (ITS) Manager of Application Support and the two ITS Senior Programmer Analysts had the ability to update all 11 forms contrary to an appropriate separation of end-user and technical support functions.

The ability to update critical student information on the 11 forms was more appropriate for College employees with Student Services and Enrollment Management responsibilities and functions that included registrar, financial aid, academic advising, and enrollment services. Further analysis of the access privileges granted to the three ITS employees disclosed the assignment of a Banner® ERP system-delivered class that allowed the ability to update all forms within the student module. The class, according to College management, had been assigned to facilitate processing support for the end users and for implementing vendor-provided corrections. Notwithstanding the need for ITS employees to update Banner® ERP system data under certain circumstances, or the ability to record changes made by each employee, the ITS employees' daily responsibilities did not require complete update access privileges to student information within the Banner® ERP system.

In response to our inquiry, College management indicated that the access privileges granted to the 11 forms and the delivered class had been removed from the ITS Manager of Application Support as of December 2019. In addition, management indicated that, as of July 2020, the existing update access privileges to critical student information had been removed for the two ITS Senior Programmer Analysts and that future update access privileges to this information would be granted on a temporary, as-needed basis by the student data custodian.

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

Recommendation: We recommend that College management continue 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.

Finding 2: Security Controls – 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 related to 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 account 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 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 2019 through July 2020 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 March 2019 through December 2019, 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.

In planning and conducting our audit, we identified internal controls significant to our audit objectives by considering the internal control integrated framework established by the Committee of Sponsoring Organizations (COSO)¹ and adapted for a government environment within the *Standards for Internal Control in the Federal Government* issued by the United States Government Accountability Office. That framework is illustrated in the following table.

¹ The Committee of Sponsoring Organizations (COSO) of the Treadway Commission was established in 1985 to develop guidance in the areas of risk and control which enable good organizational governance and reduction of fraud. Pursuant to their mission, COSO developed a framework for internal control that consists of five components and 17 underlying principles.

COSO Internal Control Integrated Framework

Internal Control Component	Description	Underlying Principles (To be Applied by the Board and College Management)
Control Environment	Standards, processes, and structures that provide the basis for carrying out internal control across the organization. Represents the foundation on which an effective internal control system is built.	<ul style="list-style-type: none"> • Demonstrate commitment to integrity and ethical values. • Exercise oversight responsibility. • Establish structures and reporting lines and assign authorities and responsibilities. • Demonstrate commitment to a competent workforce. • Hold individuals accountable for their responsibilities.
Risk Assessment	Management's process to consider the impact of possible changes in the internal and external environment and to consider actions to mitigate the impact. The basis for how risks will be managed.	<ul style="list-style-type: none"> • Establish clear objectives to define risk and risk tolerances. • Identify, analyze, and respond to risks. • Consider the potential for fraud. • Identify, analyze, and respond to significant changes that impact the internal control system.
Control Activities	Activities in the form of policies, procedures, and standards that help management mitigate risks. Control activities may be preventive in nature or detective in nature and may be performed at all levels of the organization.	<ul style="list-style-type: none"> • Design control activities to achieve objectives and respond to risks. • Design control activities over technology. • Implement control activities through policies and procedures.
Information and Communication	Information obtained or generated by management to support the internal control system. Communication is the dissemination of important information to help the organization meet requirements and expectations.	<ul style="list-style-type: none"> • Use relevant and quality information. • Communicate necessary information internally to achieve entity objectives. • Communicate necessary information externally to achieve entity objectives.
Monitoring	Periodic or ongoing evaluations to verify that the internal control system is present and functioning properly.	<ul style="list-style-type: none"> • Conduct periodic or ongoing evaluations of the internal control system. • Remediate identified internal control deficiencies on a timely basis.

We determined that all internal control components were significant to our audit objectives. The associated underlying principles significant to our objectives included:

- College and management commitment to integrity and ethical values.
- Board exercise of oversight responsibility.
- Management establishment of an organizational structure, assignment of responsibility, and delegation of authority to achieve the College's goals and objectives.
- Management identification and analysis of and response to risks.
- Management design of control activities to achieve the College's objectives and respond to risks.
- Management design of controls over information technology.
- Management establishment of policies and procedures to implement internal control activities.
- Management use of relevant and quality information to achieve the College's objectives.
- Management communication of information internally necessary to achieve the College's objectives.
- Management communication of information externally necessary to achieve the College's objectives.
- Management activities to monitor the College's internal control system and evaluate the results.
- Management remediation of identified internal control deficiencies on a timely basis.

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.
- To evaluate 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, and the database management system; Banner® ERP system application change management; device management; and the information security program addressing student records and information, including the program coordinator designation.
- Evaluated the effectiveness of logical access controls, including the periodic reviews of accounts assigned to the network domain, application and database servers, and database management system supporting the Banner® ERP system.
- Evaluated effectiveness of logical controls assigned within the Banner® ERP system, including periodic reviews.
- Examined and evaluated the appropriateness of administrative access privileges for the College's network domain as of September 30, 2019.

- Examined and evaluated the 3 domain accounts, as of October 23, 2019, not required to have a password change.
- Examined and evaluated the appropriateness of access privileges granted on the ten servers supporting the Banner® ERP system. Specifically, we examined:
 - The 54 accounts assigned on the database server supporting the Banner® ERP system as of September 30, 2019.
 - Accounts for eight application servers as of September 30, 2019. Specifically, the 34 accounts assigned to three servers, the 32 accounts assigned to three other servers, the 33 accounts assigned to another server, and the 31 accounts assigned to the eighth server.
 - The 58 accounts assigned to the job submission server as of September 30, 2019.
- Examined and evaluated the appropriateness of accounts and privileges to the database supporting the Banner® ERP system. Specifically, we examined and evaluated:
 - The 136 accounts with selected administrative access privileges as of September 30, 2019.
 - The 16 accounts with default passwords assigned as of September 30, 2019.
- 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 23, 2019, granted within the Banner® ERP system for the 78 employees assigned 11 forms.
- Evaluated College procedures related to Banner® ERP system patches, upgrades, and data fixes to determine whether the College's change management controls are designed to ensure the appropriate authorization, testing, and approval of Banner® ERP system changes.
- Examined selected database and server logs to determine the adequacy of the College's logging and monitoring controls designed for the infrastructure supporting the Banner® ERP system, including actions performed by privileged users.
- Examined selected procedures, logs, and change requests related to the IT infrastructure applicable to the Banner® ERP system to determine whether the College's system software and network infrastructure component change control procedures were designed in accordance with IT best practices.
- Examined selected reports and documents for recorded changes to confidential and critical student records and application table changes to determine the adequacy of the College's logging and monitoring controls related to student information within the Banner® ERP system.
- Examined selected scan reports, audit policies, logs, alert messages, and documents to evaluate the adequacy of the College's controls for vulnerability management 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 procedures related to the College's mobile device security plan, including security and configuration requirements and College and user-defined responsibilities, to determine the adequacy of controls for managing mobile devices connected to the College's network or used to store confidential and sensitive data.
- Examined selected documents and records related to the College's 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.

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



STATE COLLEGE OF FLORIDA, MANATEE-SARASOTA

OFFICE OF THE PRESIDENT
Carol F. Probstfeld, Ed.D.

September 23, 2020

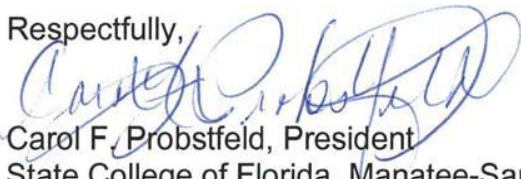
Sherrill F. Norman, CPA
Auditor General
3505 East Frontage Rd, Suite 350
Tampa, FL 33607

Dear Ms. Norman:

In response to your letter dated September 10, 2020 regarding the Information technology operational audit of the State College of Florida, Manatee-Sarasota Ellucian Banner® Enterprise Resource Planning System, please find attached a written statement of explanation and the corrective actions to the Preliminary and Tentative Audit Findings.

Please let me know if you have questions or need additional information.

Respectfully,


Carol F. Probstfeld, President
State College of Florida, Manatee-Sarasota
5840 26th Street West
Bradenton, Florida 34207

scf.edu • Mailing Address: P.O. Box 1849 Bradenton, FL 34206 • Office Phone: 941-752-5201

SCF BRADENTON
5840 26th Street West • 941-752-5000

SCF LAKEWOOD RANCH
7131 Professional Parkway East • 941-363-7000

SCF VENICE
8000 South Tamiami Trail • 941-408-1300



STATE COLLEGE OF FLORIDA, MANATEE-SARASOTA

OFFICE OF THE PRESIDENT
Carol F. Probstfeld, Ed.D.

STATE COLLEGE OF FLORIDA, MANATEE-SARASOTA

**RESPONSE TO PRELIMINARY AND TENTATIVE AUDIT FINDINGS AND
RECOMMENDATIONS**

**INFORMATION TECHNOLOGY OPERATIONAL AUDIT
ELLUCIAN BANNER® ENTERPRISE RESOURCE PLANNING.**

The following is the State College of Florida, Manatee-Sarasota (SCF) response to the findings identified in the State Auditor General's Information Technology Operational Audit Report.

RESPONSE TO FINDINGS AND RECOMMENDATIONS

Finding No. 1: Access Privileges

Recommendation: We recommend that College management continue 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.

College Response:

Permanent modify access privileges has been removed, however, modify access will be granted on a temporary basis, as needed, by the student data custodian.

Finding No. 2: Security Controls - Account Management

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

College Response:

SCF's IT security team will continue to do formal access reviews for all critical systems on a regular basis to ensure that security controls related to account management are appropriate and necessary.

scf.edu • Mailing Address: P.O. Box 1849 Bradenton, FL 34206 • Office Phone: 941-752-5201

SCF BRADENTON
5840 26th Street West • 941-752-5000

SCF LAKEWOOD RANCH
7131 Professional Parkway East • 941-363-7000

SCF VENICE
8000 South Tamiami Trail • 941-408-1300