STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2020-130
February 2020

FLORIDA SOUTHWESTERN STATE COLLEGE

Ellucian Banner® Enterprise Resource Planning System

Sherrill F. Norman, CPA
Auditor General

Board of Trustees and President

During the period, October 2018 through July 2019, Dr. Jeffery S. Allbritten served as President of Florida SouthWestern State College and the following individuals served as Members of the Board of Trustees:

	County
Braxton C. Rhone, Chair through 5-28-19 [a]	Lee
Danny Nix Jr., Vice Chair through 5-28-19, Chair from 5-29-19	Charlotte
Christian Cunningham, Vice Chair from 5-29-19	Collier
Mike Boose through 3-8-19 [b]	Collier
David Ciccarello from 7-31-19	Lee
Bruce Laishley	Charlotte
Jonathan A. Martin	Lee
Laura Perry	Glades
Julia du Plooy	Hendry
Marjorie Starnes-Bilotti	Lee

[a] Trustee position vacant through 7-30-19.
[b] Trustee position vacant from 3-9-19.

The team leader was Joseph D. Garcia, 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

FLORIDA SOUTHWESTERN STATE COLLEGE

Ellucian Banner® Enterprise Resource Planning System

SUMMARY

This operational audit of Florida SouthWestern 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, 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: College controls related to application security management need improvement to ensure that access privileges related to student information granted within the Banner® ERP system are necessary and appropriate.

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

BACKGROUND

Florida SouthWestern 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 for recording, processing, and reporting finance, human resources, and student-related transactions. 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: 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 measures that restrict the access privileges granted to employees to only those necessary for assigned responsibilities or functions. Such access controls are essential to protect the confidentiality, integrity, and availability of data and IT resources. Appropriately restricted access privileges help protect data and IT resources from unauthorized modification, loss, or disclosure. In addition, periodic reviews of employee access privileges help ensure that access privileges granted to employees remain appropriate and necessary.

Forms are screens or pages used to record information in the Banner® ERP system. Access privileges granted to a form allow the user access to all data fields and tabs within the form and security is based on assigning the forms to user classes and roles. As part of our audit procedures, we identified seven forms that allowed access to College-defined confidential and critical student data. Our examination of the access privileges for 150 Banner® ERP system users assigned 1 or more of the 7 forms indicated that 18 employee accounts with access privileges to selected student information were unnecessary. Specifically,

- The accounts assigned to 2 student employees had access privileges that allowed the employees the ability to view and update current and historical student information such as status, student type, residence, fee rate, and program and major. In addition, an account assigned to an Academic Support Programs staff assistant had access privileges granted that allowed the staff assistant the ability to view and update test score information related to college entrance exams and program requirements. These access privileges were unnecessary for the 3 employees' assigned responsibilities. Subsequent to our audit inquiry, College management indicated that access privileges for the 3 employee accounts were changed to inquiry only.
- Although unnecessary for the employees' assigned responsibilities, 15 accounts assigned to employees in various student-related positions, including admissions, student services, advising, and instruction; student employees; a Marketing Coordinator; and an accountant had access privileges granted that allowed the employees the ability to view and update student information such as course registration, fees, residency status, grades, test scores, and biographical information. In response to our audit inquiry, College management indicated that the access privileges for all 15 employee accounts were either removed or changed to inquiry only, as appropriate.
- As of October 2019, the College had not performed a comprehensive review of employee access privileges related to student information granted within the Banner® ERP system. In response to our audit inquiry, College management indicated that the former Registrar was performing such a review prior to his unexpected departure in March 2019 and that a review of Banner® ERP system accounts and associated student access privileges was currently in process under the new Registrar hired in August 2019.

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

Recommendation: We recommend that College management 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 that periodic reviews of the access privileges granted are performed.

Finding 2: Security Controls – User Authentication and Network 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 user authentication and network 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 and network 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 the IT security controls related to user authentication and network 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 May 2019 through September 2019 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 Ellucian Banner® Enterprise Resource Planning (Banner® ERP) system for maintaining and processing student account information, on the College's compliance with the Safeguards Rule, and the Banner® ERP system supporting infrastructure during the period October 2018 through July 2019 and selected actions thereto. The overall objectives of the audit were:

- To evaluate 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 and controls included within the scope of the audit, deficiencies in management's internal controls; 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 and controls 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 the IT systems and 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:

- Interviewed College staff and reviewed College records to obtain an understanding of and evaluate College operations for the Banner® ERP system infrastructure, including authentication and logging and monitoring of the network, application and database servers, and the database management system; Banner® application logical controls, change management, and logging and monitoring; vulnerability management; device management for personally owned mobile devices connecting to the College's network; 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 for the network domain, application and database servers, and database supporting the Banner® ERP system.
- Examined and evaluated the appropriateness of accounts assigned on 7 of the 12 servers supporting the Banner® ERP system. Specifically, we examined and evaluated:
  - 31 accounts assigned to 1 of 3 administration servers as of May 24, 2019.
  - 36 accounts assigned to the programming interface server as of May 24, 2019.
  - 71 accounts assigned to the database server as of May 24, 2019.
  - 35 accounts assigned to the finance application server as of May 24, 2019.
  - 34 accounts assigned to the HR application server as of May 24, 2019.
  - 25 accounts assigned to the database management server as of May 24, 2019.
  - 34 accounts assigned to 1 of 4 student application servers as of May 24, 2019.
- Examined and evaluated the appropriateness of accounts and privileges granted to the database. Specifically, we examined and evaluated:
  - 229 accounts that were assigned selected administrative privileges as of May 24, 2019.
  - 25 accounts with database privileges that allowed direct database sign-on as of May 24, 2019.
  - 26 accounts with default passwords as of June 14, 2019.
- Examined and evaluated 587 network domain accounts, as of May 20, 2019, not required to have a password change.

- Examined and evaluated the appropriateness of administrative privileges, as of May 20, 2019, for the College's network domain.
- Examined seven selected student records forms and evaluated the appropriateness of user access privileges granted to these forms within the Banner® ERP system as of May 24, 2019.
- Examined four selected student revenue transaction forms and evaluated the appropriateness of user access privileges granted to these forms within the Banner® ERP system as of May 24, 2019.
- Evaluated the effectiveness of logical access controls, including the periodic reviews of access privileges assigned within the Banner® ERP system related to confidential student records and student revenue transactions.
- Evaluated user authentication controls related to accessing the Banner® ERP system student application.
- Evaluated user authentication controls related to the College's IT Infrastructure supporting the Banner® ERP system.
- Evaluated the College's information security program over student records.
- Evaluated the effectiveness of the College's logging and monitoring controls related to confidential student records and student revenue transactions in the Banner® ERP system.
- Evaluated the effectiveness of the College's logging and monitoring controls related to the College's database server and database supporting the Banner® ERP system.
- Evaluated the effectiveness of the College's controls for managing mobile devices (e.g., user provisioning and incident response management), layered security controls (e.g., hardening guidelines, malware protection, data security such as encryption, and access controls) and security awareness controls (e.g., user training and policies and procedures).
- Evaluated the effectiveness of the College's vulnerability management (logging, monitoring, and remediation) for the network and critical network infrastructure supporting the Banner® ERP system.
- Evaluated the effectiveness of the College's change management controls related to approving, testing, and implementing infrastructure system software changes.
- Evaluated the effectiveness of the College's change management controls related to approving, testing, and implementing Banner® ERP system changes.
- 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***.

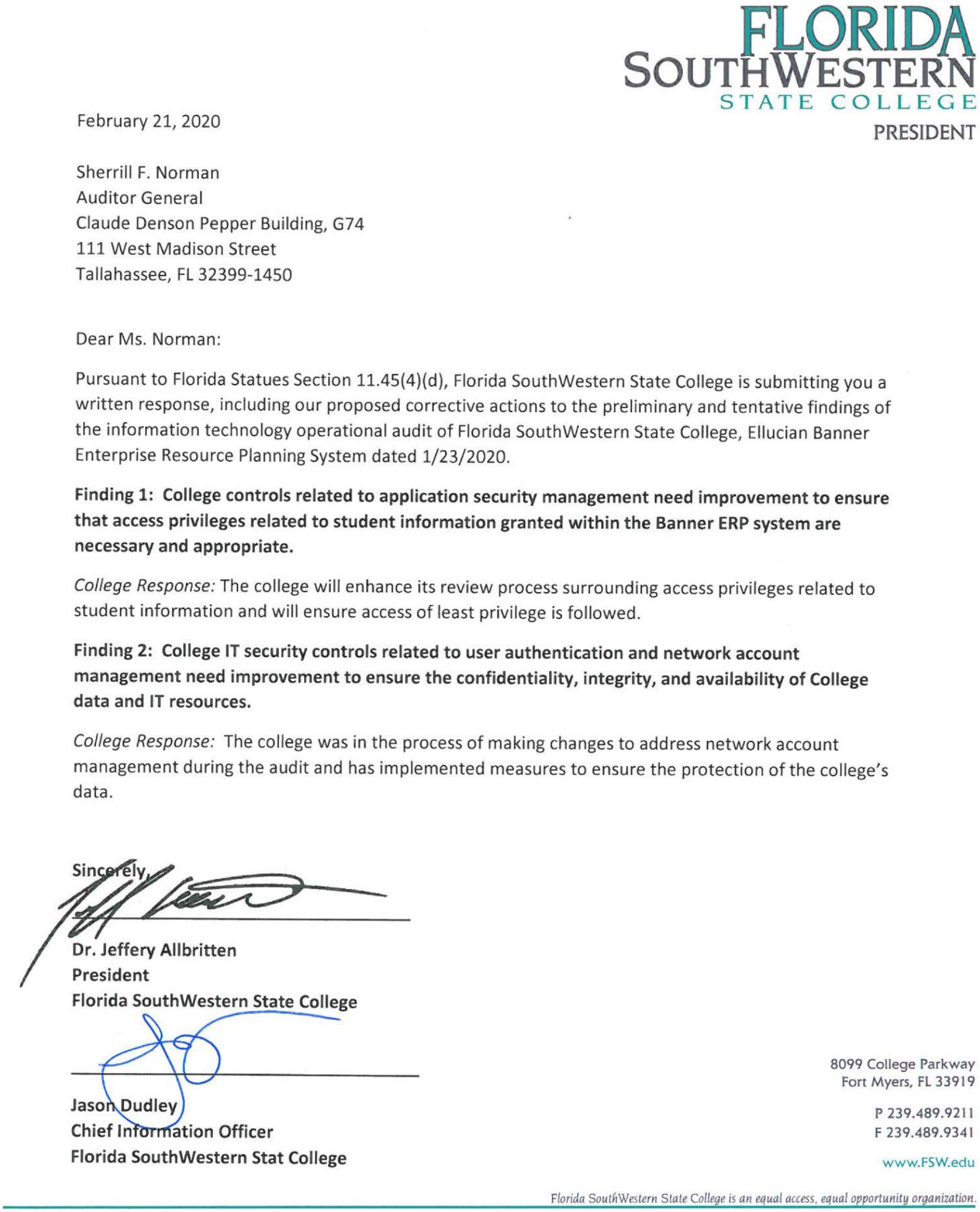
AUTHORITY

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

Sherrill F. Norman, CPA
Auditor General

MANAGEMENT'S RESPONSE



FLORIDA
SOUTHWESTERN
STATE COLLEGE
PRESIDENT

February 21, 2020

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

Dear Ms. Norman:

Pursuant to Florida Statues Section 11.45(4)(d), Florida SouthWestern State College is submitting you a written response, including our proposed corrective actions to the preliminary and tentative findings of the information technology operational audit of Florida SouthWestern State College, Ellucian Banner Enterprise Resource Planning System dated 1/23/2020.

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

College Response: The college will enhance its review process surrounding access privileges related to student information and will ensure access of least privilege is followed.

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

College Response: The college was in the process of making changes to address network account management during the audit and has implemented measures to ensure the protection of the college's data.

Sincerely,

Dr. Jeffery Allbritten
President
Florida SouthWestern State College

Jason Dudley
Chief Information Officer
Florida SouthWestern Stat College

8099 College Parkway
Fort Myers, FL 33919

P 239.489.9211
F 239.489.9341

www.FSW.edu

Florida SouthWestern State College is an equal access, equal opportunity organization.