STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2019-043
October 2018

SOUTH FLORIDA STATE COLLEGE

Ellucian Banner® Enterprise Resource Planning System

Sherrill F. Norman, CPA
Auditor General

Board of Trustees and President

During the period, March 2018 through June 2018, Dr. Thomas C. Leitzel served as President of South Florida State College and the following individuals served as Members of the Board of Trustees:

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

SOUTH FLORIDA STATE COLLEGE

Ellucian Banner® Enterprise Resource Planning System

SUMMARY

This operational audit of South Florida 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's Banner® ERP system. Our audit disclosed the following:

Finding 1: The College's security management over confidential and sensitive student records information within the Banner ERP® system needs improvement.

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

BACKGROUND

South 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 Education rules. A Board of Trustees (Board) governs and operates the College. The Board constitutes a corporation and is composed of eight 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: Security Management

Effective application security management provides a framework for managing risk, developing security policies, and monitoring the adequacy of application-related controls. Preserving authorized restrictions on information access and disclosure through access controls and security design is an essential component of managing security over the confidentiality of data.

Forms are screens or pages used to record information in the Banner® ERP system. Security is based on controlling a user's access to these forms. Access privileges granted to a form allows the user access to all data fields and tabs within the form unless additional security measures have been set, such as the use of masking where specific, sensitive data can be protected at the field level.

Our audit procedures disclosed that the College did not have additional security measures set within the Banner® ERP system student records forms to restrict access to confidential or sensitive data and did not have policies and procedures in place to evaluate and document users' need for access to all confidential or sensitive information, such as social security numbers and demographic, admissions, registration, grades, and academic standing data, present within the forms when granting access. In response to our audit inquiry, College management indicated that access to the forms would be removed and that going forward, access to the forms would be provided only as approved by the security team based on documented need for access. In addition, management indicated that the College is in the process of building masking rules for certain data fields.

Appropriately managing the security over confidential or sensitive data helps protect data from unauthorized disclosure.

Recommendation: We recommend that College management improve security management over confidential and sensitive student records information within the Banner® ERP system through restriction of access privileges and added security measures, as appropriate.

Finding 2: Security Controls – User Authentication, User Account Management, and Monitoring

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, user account management, and monitoring 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, user account management, and monitoring, the risk is increased that the confidentiality, integrity, and availability of College data and related IT resources may be compromised.

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

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of educational 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 March 2018 through June 2018 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 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 March 2018 through June 2018. 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 records 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 College management and staff 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® ERP system application change 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 for the network domain, application and database servers, and database supporting the Banner® ERP system.
- Examined and evaluated the appropriateness of 54 accounts and 4 services assigned to the database server as of March 23, 2018.
- Examined and evaluated the appropriateness of accounts and privileges granted to the database. Specifically, we examined and evaluated:
  - 75 accounts that were assigned selected administrative privileges as of March 23, 2018.
  - 33 accounts with database privileges that allowed direct database sign-on as of March 23, 2018.
  - 30 accounts with default passwords assigned as of April 9, 2018.
- Examined and evaluated the appropriateness of administrative privileges, as of March 23, 2018, for the College's network domain and application server.
- Examined and evaluated 33 network domain accounts, as of March 23, 2018, not required to have a password change.
- Examined eight selected student records forms and evaluated the appropriateness of user update access privileges granted to these forms within the Banner® ERP system as of March 5, 2018.
- Examined eight selected student records forms and evaluated the appropriateness of user inquiry access privileges granted to these forms within the Banner® ERP system as of March 5, 2018.
- Examined four selected student receivable transactions and evaluated the appropriateness of the user access privileges granted to these transactions within the Banner® ERP system as of March 5, 2018.
- Evaluated the effectiveness of logical access controls, including the periodic reviews of access privileges assigned within the Banner® ERP system related to student receivables and student records.
- Evaluated user authentication controls related to accessing the Banner® ERP system student receivables and student records.
- 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 student receivable and student record 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 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 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***.

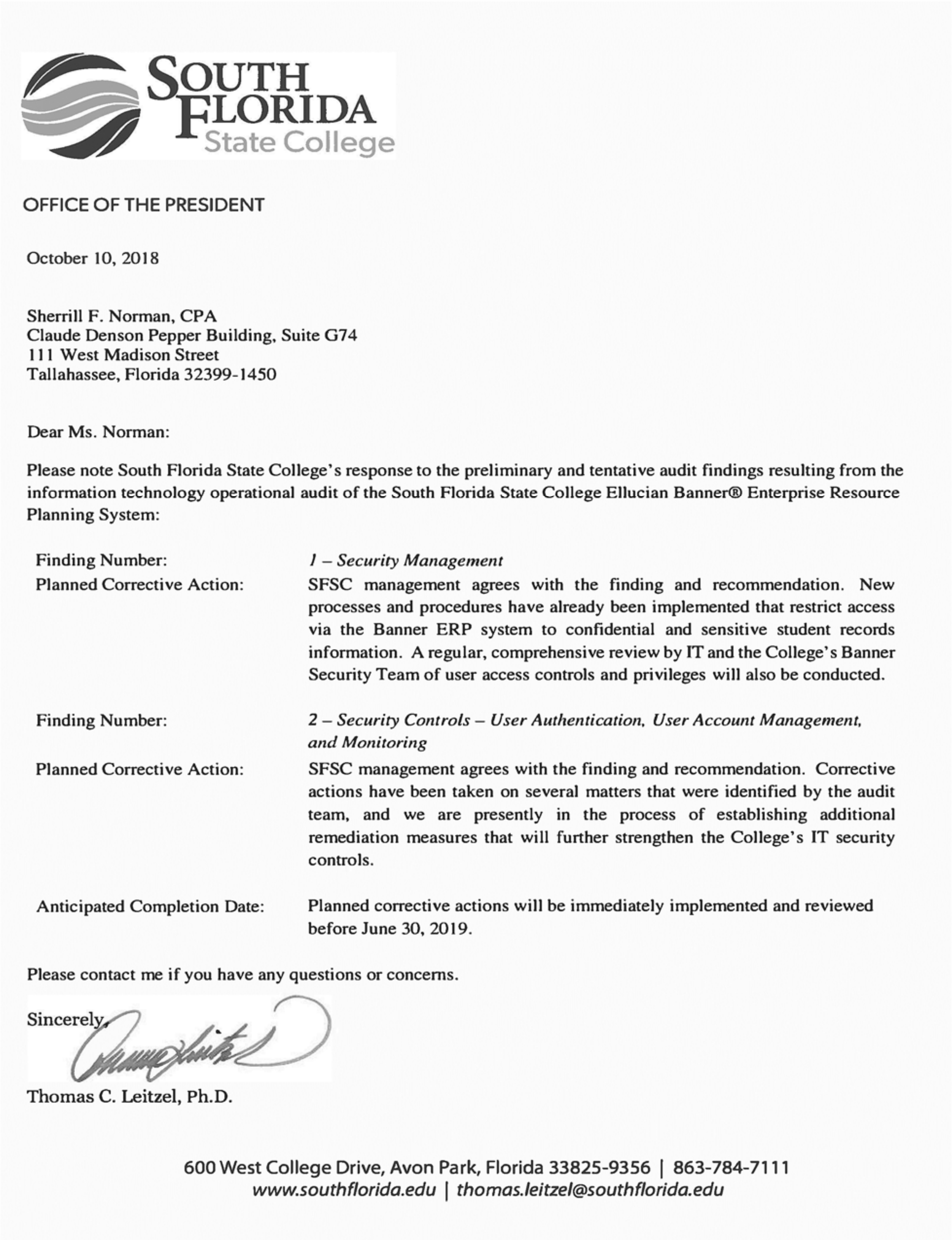
AUTHORITY

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



OFFICE OF THE PRESIDENT

October 10, 2018

Sherrill F. Norman, CPA
Claude Denson Pepper Building, Suite G74
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Ms. Norman:

Please note South Florida State College’s response to the preliminary and tentative audit findings resulting from the information technology operational audit of the South Florida State College Ellucian Banner® Enterprise Resource Planning System:

Finding Number:	*1 – Security Management*
Planned Corrective Action:	SFSC management agrees with the finding and recommendation. New processes and procedures have already been implemented that restrict access via the Banner ERP system to confidential and sensitive student records information. A regular, comprehensive review by IT and the College’s Banner Security Team of user access controls and privileges will also be conducted.
Finding Number:	*2 – Security Controls – User Authentication, User Account Management, and Monitoring*
Planned Corrective Action:	SFSC management agrees with the finding and recommendation. Corrective actions have been taken on several matters that were identified by the audit team, and we are presently in the process of establishing additional remediation measures that will further strengthen the College’s IT security controls.
Anticipated Completion Date:	Planned corrective actions will be immediately implemented and reviewed before June 30, 2019.

Please contact me if you have any questions or concerns.

Sincerely,

Thomas C. Leitzel, Ph.D.