STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2019-007
August 2018

UNIVERSITY OF WEST FLORIDA

Ellucian Banner® Enterprise Resource Planning System

Sherrill F. Norman, CPA
Auditor General

Board of Trustees and President

During the period, January 2018 through April 2018, Dr. Martha Saunders served as President of the University of West Florida and the following individuals served as Members of the Board of Trustees:

[a] Student Body President.
[b] Faculty Senate President.
[c] Trustee position vacant from 1-7-18 to 2-8-18.
[d] Trustee position vacant through 2-8-18.

The team leader was Sue Graham, CPA, 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

UNIVERSITY OF WEST FLORIDA

Ellucian Banner® Enterprise Resource Planning System

SUMMARY

This operational audit of the University of West Florida (University) 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 and on the University's compliance with the Federal Trade Commission's Standards for Safeguarding Customer Information (Safeguards Rule). Our audit disclosed the following:

Finding 1: Some University employees' Banner® ERP system access privileges to student records were unnecessary for the employees' assigned job responsibilities.

Finding 2: The University did not perform a periodic review of Banner® ERP system access privileges to student receivables and student records.

Finding 3: The University had not completed a formal risk assessment as part of the comprehensive information security program necessary for compliance with the Safeguards Rule. In addition, some controls implemented to address areas of risk related to securing customer information need improvement.

Finding 4: University IT security controls related to user authentication and monitoring of system activity need improvement.

BACKGROUND

The University of West Florida (University) is part of the State university system of public universities, which is under the general direction and control of the Florida Board of Governors (BOG). The University is directly governed by a Board of Trustees (Trustees) consisting of 13 members. The Governor appoints 6 citizen members and the BOG appoints 5 citizen members. These members are confirmed by the Florida Senate and serve staggered 5-year terms. The Faculty Senate President and Student Body President also serve as members.

While the BOG establishes the powers and duties of the Trustees, the Trustees are responsible for setting University policies, which are to provide governance in accordance with State law and BOG regulations. The Trustees select the University President, who is subject to confirmation by the BOG. The University President serves as the executive officer and the corporate secretary of the Trustees and is responsible for administering the University policies prescribed by the Trustees.

The University 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 University is defined as a financial institution by the Federal Trade Commission and, therefore, is subject to the provisions of the Gramm-Leach-Bliley Act.

FINDINGS AND RECOMMENDATIONS

Finding 1: Access Privileges

Access controls are intended to protect data and 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.

University employees' access privileges to selected student record information within the Banner® ERP system, including demographics, admissions, and registration, were unnecessary for some employees' assigned responsibilities. Specifically, our test of 128 employees' update access to selected student record information disclosed that, although not required to perform their assigned job duties, 5 employees within the Controller's Office had the ability to update admissions applications. Subsequent to our audit inquiry, University management indicated that the 5 employees' unnecessary access privileges were removed.

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

Recommendation: We recommend that University management ensure that employee access privileges granted within the Banner® ERP system for student records are necessary for the employees' assigned responsibilities.

Finding 2: Periodic Review of Access Privileges

Effective access controls include periodic reviews of employee access privileges granted to business data to help ensure that only authorized employees have access and that the access provided to each employee remains appropriate and necessary for the employee's assigned job duties.

The University uses groups to grant access privileges to users within the Banner® ERP system. Written procedures have been established to require the semiannual review by security managers (module owners) of user access privileges granted within the Banner® ERP system for student receivables and student records. Our audit procedures disclosed, however, that the security managers had not performed reviews of user access privileges nor had they performed periodic reviews of access privileges associated with groups to ensure that the groups continued to remain appropriate. In addition, although biweekly reports of employee terminations and transfers were provided to security managers for review, the reports did not include the University's work study students employed in positions that changed from term to term. In response to our audit inquiry, University management indicated that an automated notification will be sent to security managers reminding them of their responsibility to review user access privileges and that an annual process requiring a review of the groups and the assigned access privileges will be established. Further, management indicated that a process would be determined to best review the access privileges granted to work study students given the significant number of positions and changes that occur.

Periodic reviews of user access privileges for student receivables and student records increase management's assurance that user access privileges continue to be authorized and appropriate and reduce the risk that unauthorized disclosure, modification, or destruction of University-maintained data may occur.

Recommendation: We recommend that University management perform periodic reviews of the access privileges granted within the Banner® ERP system for student receivables and student records to verify that the access privileges are appropriate.

Finding 3: Information Security Program

Standards for Safeguarding Customer Information[1] (Safeguards Rule), issued by the Federal Trade Commission as required by the Gramm-Leach-Bliley Act, require the development, implementation, and maintenance of a comprehensive information security program that includes reasonable administrative, technical, and physical safeguards to secure customer information (i.e., nonpublic personal information) and to regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

A comprehensive information security program includes designating an employee, or employees, to coordinate the institution's information security program, completing a risk assessment, and designing and implementing key controls and procedures identified through risk assessment. Identification of internal and external risks to the security, confidentiality, and integrity of customer information by the institution gives consideration of risk in each relevant area of the institution's operations such as employee training and management; applicable systems and information processing, storage, transmission; and incident determination, reporting, and response.

Although the University designated an Information Security Program Coordinator and developed an incident response program, the University had not completed a formal risk assessment of the systems applicable to the processing, storage, and transmission of customer information. In addition, controls implemented to address University management's consideration of certain areas of risk related to securing customer information need improvement. Specifically, our audit disclosed that:

- Although the University addressed the protection of confidential information in its security awareness training provided to University employees in 2016 and subsequently to new hires, the University did not provide continued, periodic security awareness training to ensure employees' understanding of regulations, policies, and potential threats and acknowledgement of responsibilities.
- The *University of West Florida Information and Security Privacy Policy* (*Policy*) requires authorization for the storage of protected information on University-owned portable computing or storage devices or personal computing devices and for the transfer of protected information. Such authorization should be documented and maintained in accordance with the *Policy*. Notwithstanding the defined *Policy*, University management did not have procedures in place to ensure that appropriate authorizations are being made.
- Although the *Policy* addresses encryption for authorized storage and transfer of protected information, the requirement for data encryption is limited to social security numbers.

[1] Title 16, Section 314, Code of Federal Regulations.

In response to our audit inquiry, University management indicated that a risk assessment process for each of the University's critical systems is being developed.

A comprehensive information security program, including a formal risk assessment and the design and implementation of appropriate mitigating controls, demonstrates University management's compliance with the Safeguards Rule and supports the University's obligation to protect the security, confidentiality, and integrity of customer information.

Recommendation: We recommend that University management complete a formal risk assessment as part of the comprehensive information security program necessary for compliance with the Safeguards Rule. In addition, University management should improve controls over securing customer information, including controls related to employee security awareness training, authorization for storage and transfer of data, and data encryption requirements.

Finding 4: Security Controls – User Authentication 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 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 University data and related IT resources. However, we have notified appropriate University management of the specific issues.

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

Recommendation: We recommend that the University improve IT security controls related to user authentication and monitoring to ensure the confidentiality, integrity, and availability of University 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 January 2018 through April 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 University IT controls primarily applicable to the Banner® ERP system for maintaining and processing student account information and on the University's compliance with the Safeguards Rule during the period January 2018 through April 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 University 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 University staff and reviewed operational documentation to obtain an understanding of and evaluate the University's information security program addressing student records and information and designating a coordinator for the program.
- Examined four selected student receivable transactions and evaluated the appropriateness of the user access privileges granted, as of January 5, 2018, to these transactions within the Banner® ERP system.
- Examined eight selected student records transactions and evaluated the appropriateness of user access privileges, as of January 3, 2018, granted within the Banner® ERP system.
- Examined ten selected student records transactions and evaluated the appropriateness of eight University work study students' access privileges, as of January 3, 2018, granted within the Banner® ERP system.

- Evaluated user authentication controls related to accessing Banner® ERP system student receivables and student records.
- Evaluated the effectiveness of logical access controls, including periodic reviews of access privileges assigned within the Banner® ERP system related to student receivables and student records.
- Evaluated the University's information security program over student records.
- Evaluated University controls for logging and monitoring student receivable and student record transactions in the Banner® ERP system.
- Evaluated University controls for logging and monitoring the actions of privileged database users in the Banner® ERP system.
- 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***.

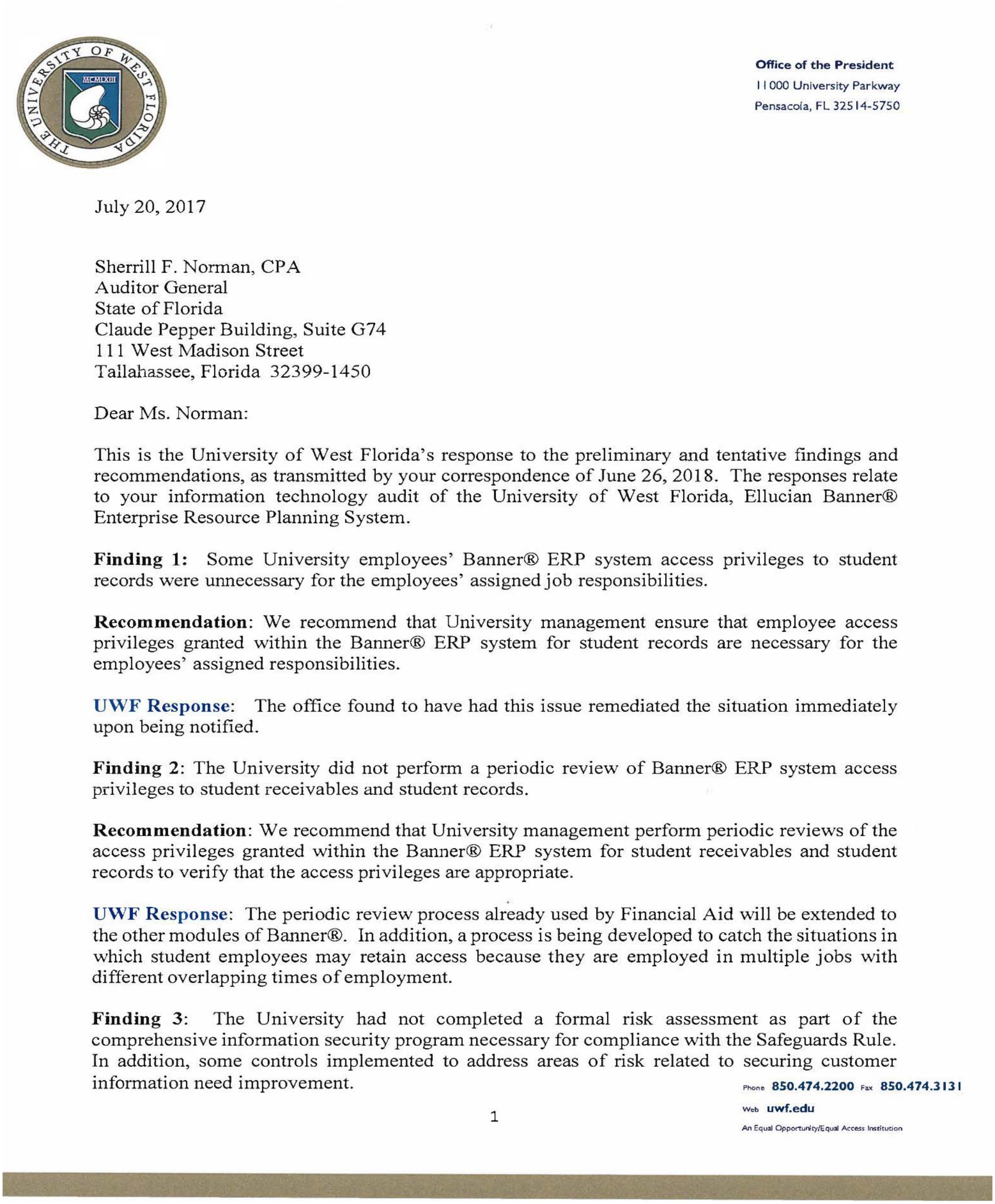
AUTHORITY

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
11000 University Parkway
Pensacola, FL 32514-5750

July 20, 2017

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

Dear Ms. Norman:

This is the University of West Florida's response to the preliminary and tentative findings and recommendations, as transmitted by your correspondence of June 26, 2018. The responses relate to your information technology audit of the University of West Florida, Ellucian Banner® Enterprise Resource Planning System.

Finding 1: Some University employees' Banner® ERP system access privileges to student records were unnecessary for the employees' assigned job responsibilities.

Recommendation: We recommend that University management ensure that employee access privileges granted within the Banner® ERP system for student records are necessary for the employees' assigned responsibilities.

UWF Response: The office found to have had this issue remediated the situation immediately upon being notified.

Finding 2: The University did not perform a periodic review of Banner® ERP system access privileges to student receivables and student records.

Recommendation: We recommend that University management perform periodic reviews of the access privileges granted within the Banner® ERP system for student receivables and student records to verify that the access privileges are appropriate.

UWF Response: The periodic review process already used by Financial Aid will be extended to the other modules of Banner®. In addition, a process is being developed to catch the situations in which student employees may retain access because they are employed in multiple jobs with different overlapping times of employment.

Finding 3: The University had not completed a formal risk assessment as part of the comprehensive information security program necessary for compliance with the Safeguards Rule. In addition, some controls implemented to address areas of risk related to securing customer information need improvement.

Recommendation: We recommend that University management complete a formal risk assessment as part of the comprehensive information security program necessary for compliance with the Safeguards Rule. In addition, University management should improve controls over securing customer information, including controls related to employee security awareness training, authorization for storage and transfer of data, and data encryption requirements.

UWF Response: A formal risk assessment will be completed to successfully comply with the Safeguards Rule. Ongoing security awareness training has begun (Phishing awareness/testing/training), and awareness campaigns covering key security principles will be delivered throughout the year. The Information Security and Privacy Policy is being updated to make the transfer of Protected data onto portable data storage devices a violation of the policy; this also obviates the need to use encryption on those devices. Access to Protected data will only be allowed through secure network access instead.

Finding 4: University IT security controls related to user authentication and monitoring of system activity need improvement.

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

UWF Response: UWF has deployed Multi-Factor authentication for all Banner® ERP privileged account access to the system. ITS will create automated triggers which will monitor database logs and alert all DBAs and the Director of Infrastructure Services upon specific high-privilege actions taken on the Banner® ERP database.

We appreciate the constructive assistance that the Auditor General provides to us and will work toward the timely implementation of these recommendations.

Sincerely yours,

Martha Saunders

Martha D. Saunders, Ph.D.
President

cc: Mr. Mort O'Sullivan, UWF BOT Chairman
Mr. Robert Jones, UWF BOT Audit & Compliance Committee
Mr. Dick Baker, UWF BOT Audit & Compliance Committee
Mr. Robert Sires, UWF BOT Audit & Compliance Committee
Dr. George Ellenberg, Provost/Sr. Executive Vice President
Ms. Pamela Langham, General Counsel
Ms. Melanie Haveard, Chief Technology Officer
Mr. Geissler Golding, CISO
Ms. Cynthia Talbert, Interim Internal Audit Director