STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2021-212
May 2021

UNIVERSITY OF SOUTH FLORIDA

Ellucian Banner® Student System and Prior Audit Follow-Up

Sherrill F. Norman, CPA
Auditor General

Board of Trustees and President

During the period October 2019 through August 2020, Dr. Steven C. Currall served as President of the University of South Florida and the following individuals served as Members of the Board of Trustees:

Jordan B. Zimmerman, Chair
Stephanie E. Goforth, Vice Chair from 6-3-20
Leslie M. Muma, Vice Chair through 6-2-20
Dr. Timothy L. Boaz from 8-10-20 [a]
Sandra Callahan
Michael Carrere
Michael E. Griffin
Britney Deas through 5-10-20 [b]
Oscar J. Horton
Dr. Deanna Michael through 8-09-20 [a]
Claire Mitchel from 5-11-20 [b]
John B. Ramil
Byron E. Shinn
Charles Tokarz
Nancy H. Watkins

[a] System Faculty Council President (equivalent to Faculty Senate Chair referred to in Section 1001.71(1), Florida Statutes).

[b] Student Body President.

The team leader was Gina Bailey, CPA, CISA, CFE 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 SOUTH FLORIDA

Ellucian Banner® Student System and Prior Audit Follow Up

SUMMARY

This operational audit of the University of South Florida (University) focused on evaluating selected information technology (IT) controls applicable to the University of South Florida Ellucian Banner® Student System (Banner® Student) and on the progress that the University had made, or was in the process of making, in addressing the findings in our report No. 2017-211. Our audit disclosed the following:

Finding 1: As of June 2020, 173 of the 197 employees with IT user access privileges to update student residency status and impact student tuition assessments did not need the privileges to perform their assigned duties.

Finding 2: Certain University IT security controls related to user authentication, account management, and monitoring need improvement to ensure the confidentiality, integrity, and availability of IT resources. A similar finding was noted in our report No. 2017-211.

BACKGROUND

The University of South 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) normally 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 Chair 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® Student System (Banner® Student) for the recording, processing, and reporting of student related transactions. In addition, the Information Technology Division Data Center Infrastructure, an auxiliary of the University of South Florida Division of Information Technology, hosts Ellucian Banner® Enterprise Resource Planning (Banner® ERP) systems and provides, pursuant to agreements with other institutions, selected IT services such as hardware configuration, installation and maintenance of operating systems software, installation and maintenance of databases, and business continuity. During the period October 2019 through August 2020, the University Trustees had effective agreements with the Boards of Trustees of Florida Gulf Coast University, New College of Florida, and the University of North Florida for hosting and services related to each entity's Banner® ERP system.

FINDINGS AND RECOMMENDATIONS

Finding 1: Access Privileges

Pursuant to State law,[1] students must be classified as residents or nonresidents for the purposes of assessing tuition in postsecondary education programs offered in State universities. Appropriate access controls over student residency classifications are intended to protect data and ensure the accuracy of student tuition assessments. Such 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.

The Banner® Student SGASTDN form is the general student page or screen that allows data fields containing student information, such as residency status and curriculum information, to be updated by users with access to the form. Our examination of the access privileges as of June 2020 for all 197 Banner® Student users with access to the SGASTDN form disclosed that access privileges were not always restricted to employee assigned responsibilities. Specifically, 173 of the 197 users were authorized to update student curriculum information; however, because the 173 users had access to the form, they could update information in other data fields, including student residency status, and impact student tuition assessments.

In response to our inquiry, University management indicated that updates to student residency status are monitored and a project for implementing alternate software to update student curriculum information and further restrict the SGASTDN form is scheduled for the end of 2021.

Recommendation: University management should continue efforts to ensure that access privileges granted to update student residency status is appropriate based on employee assigned responsibilities.

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

Security controls are intended to protect the confidentiality, integrity, and availability of data and information technology (IT) resources. Our audit procedures disclosed that certain security controls related to user authentication, 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 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, account management, and monitoring, the risk is increased that the confidentiality, integrity, and availability of University data and related IT resources may be compromised. Similar findings were communicated to University management in connection with our report No. 2017-211.

[1] Section 1009.21, Florida Statutes.

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

PRIOR AUDIT FOLLOW-UP

Except for findings related to user authentication, account management, and monitoring also discussed in Finding 2 of this report, the University had taken corrective actions for findings communicated to management in connection with Finding 1 in our report No. 2017-211.

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 2020 through November 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 significant University IT controls applicable to the Ellucian Banner® Student System (Banner® Student) during the period October 2019 through August 2020, and selected actions subsequent thereto. For those areas addressed by this audit, our audit objectives 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 determine whether management has corrected, or is in the process of correcting, all deficiencies disclosed in audit report No. 2017-211.
- 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)[2] 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.

[2] 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 University 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.	• 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.	• 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.	• 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.	• 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.	• Conduct periodic or ongoing evaluations of the internal control system. • Remediate identified internal control deficiencies on a timely basis.

We determined that the internal control components significant to our audit objectives included control environment, control activities, and monitoring. The associated underlying principles significant to our objectives included:

- Board and management commitment to integrity and ethical values.
- Board exercise of oversite responsibility.
- Management establishment of an organizational structure, assignment of responsibility, and delegation of authority to achieve the University's goals and objectives.
- Management evaluation of employee performance and holding individuals accountable for their internal control responsibilities.
- Management design of control activities to achieve the University'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 University's objectives.
- Management communication of information internally necessary to achieve the University's objectives.
- Management communication of information externally necessary to achieve the University's objectives.
- Management activities to monitor the University'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, University policies and procedures, and other guidelines; interviewed University personnel; and examined University records to obtain an understanding of University operations related to Banner® Student and to evaluate whether University operations were designed properly and operating effectively.
- Evaluated the sufficiency of University controls; observed, documented, and tested key processes, procedures, and controls related to University IT processes for Banner® Student, including authentication, logical controls, logging and monitoring, and change management; evaluated the University supporting network infrastructure, including authentication and logical controls; and evaluated University management of customer Banner® ERP system infrastructure, including authentication, logical access, and logging and monitoring controls.
- Examined the Banner System Hosting and Services agreements between the University and Florida Gulf Coast University (FGCU), New College of Florida (NCF), and the University of North Florida (UNF) to determine whether responsibilities within the agreements had been clearly delineated for the University and each customer.
- Evaluated selected security settings related to the application and database servers and databases supporting Banner® Student and customer Banner® ERP systems to determine whether authentication controls were configured and enforced in accordance with IT best practices.

- Evaluated the effectiveness of logical access controls, including the periodic evaluations of University assigned accounts on the customer application and database servers.
- Evaluated the effectiveness of University processes for facilitating evaluations of FGCU, NCF, and UNF staff accounts on each respective customer's Banner® ERP system application and database servers and databases.
- Examined selected database and server logs to determine the adequacy of University logging and monitoring controls designed for the infrastructure supporting customer Banner® ERP systems, including actions performed by privileged users.
- Evaluated the effectiveness of University logical access controls assigned to the University network and application and database servers and database supporting Banner® Student, including periodic evaluations of assigned access privileges.
- Examined and evaluated security settings related to the University network to determine whether authentication controls were configured and enforced in accordance with IT best practices.
- Examined and evaluated selected services on the three customer Banner® ERP system database servers as of May 5, 2020, to determine whether the services were disabled because of known security risks.
- Examined and evaluated the appropriateness of access privileges granted on the 12 FGCU Banner® ERP system application and database servers, including:
    - The 51 accounts assigned to one or more of 11 application servers as of May 5, 2020.
    - The 88 accounts assigned to the database server as of May 5, 2020.
- Examined and evaluated the appropriateness of access privileges granted on the 7 NCF Banner® ERP system application and database servers, including:
    - The 40 accounts assigned to one or more of 6 application servers as of May 5, 2020.
    - The 59 accounts assigned to the database server as of May 5, 2020.
- Examined and evaluated the appropriateness of access privileges granted to the 9 UNF Banner® ERP system application and database servers, including:
    - The 33 accounts assigned to one or more of 8 application servers as of May 5, 2020.
    - The 62 accounts assigned to the database server as of May 5, 2020.
- Examined and evaluated the appropriateness of all accounts assigned administrative access privileges within the four default network administrator system groups for the University's root domain as of May 13, 2020.
- Examined and evaluated the 124 domain accounts not required to have a password change as of May 12, 2020.
- Examined and evaluated all 40 root accounts defined to the University and customer application and database servers not required to have a password change as of May 5, 2020.
- Evaluated the effectiveness of logical access controls within Banner® Student and reviewed University procedures related to the annual evaluation of assigned user access privileges.
- Evaluated University procedures and reviewed five change requests related to Banner® Student patches, upgrades, and data fixes and changes to supporting infrastructure, including system software and selected firewalls to determine whether modifications required appropriate authorization, testing, and approval.

- Evaluated University procedures and examined enabled database and server log information to determine the adequacy of University logging and monitoring controls designed for the infrastructure supporting Banner® Student, including actions performed by privileged users.
- Evaluated University procedures and reviewed reports related to the recording, documenting, and reporting changes to confidential and critical student record information within Banner® Student to determine the adequacy of the University's logging and monitoring controls.
- Examined and evaluated the appropriateness of access privileges granted on the Banner® Student database and 12 application and database servers, including:
  - The 40 accounts assigned to one or more of the 11 application servers as of May 5, 2020.
  - The 82 accounts assigned to the database server as of May 5, 2020.
  - The 47 accounts assigned to the database as of June 19, 2020.
- Examined and evaluated selected services on the 12 Banner® Student application and database servers as of May 5, 2020, to determine whether the services were disabled because of known security risks.
- Examined and evaluated the appropriateness of access privileges, as of June 19, 2020, granted within Banner® Student for the 1,152 accounts with access to one or more of the 40 forms granting access to confidential or critical student record fields.
- 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, CPA
Auditor General

MANAGEMENT'S RESPONSE

UNIVERSITY of SOUTH FLORIDA

May 21, 2021

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

Dear Ms. Norman,

Please find enclosed the University of South Florida response for the audit findings that were identified in the 2020 Ellucian Banner Student System and Prior Audit Follow Up administered by the State of Florida.

If you have any questions or require additional information, please contact Alex Campoe, Chief Information Security Officer, at 813-974-1796.

Sincerely,

Sidney Fernandes
Chief Information Officer
Vice President for Information Technology

Enclosure

Copy to: Dr. Steven Currall
Dr. Ralph Wilcox
David Lechner
Dr. Paul Dosal
Virginia Kalil

University of South Florida
Responses to Preliminary and Tentative Findings of the 2020
University of South Florida, Ellucian Banner Student System and Prior Audit Follow Up
conducted by the Auditor General's Office

Finding 1: Access Privileges: As of June 2020, 173 of the 197 employees with IT user access privileges to update student residency status and impact student tuition assessments did not need the privileges to perform their assigned duties.

Recommendation: University management should continue efforts to ensure that access privileges granted to update student residency status is appropriate based on employee assigned responsibilities.

Management's Response: Based on the recommendation, Information Technology was able to employ Fine Grain Access Control on the SGASTDN page in Ellucian Banner. This Fine Grain Access Control has limited access to thirteen Office of the Registrar employees who have a business need to update student residency status as part of their regularly assigned responsibilities.

Implementation Date: Friday, May 14, 2021

Responsible Party: Catherine Mund, 813-974-3777

Finding 2: Security Controls – User Authentication, Account Management, and Monitoring: Certain University IT security controls related to user authentication, account management, and monitoring need improvement to ensure the confidentiality, integrity, and availability of IT resources. A similar finding was noted in our report No. 2017-211.

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

Management's Response: As recommended, the University is putting a number of measures in place to enhance and improve our IT security controls related to user authentication, account management, and monitoring to ensure the confidentiality, integrity, and availability of IT resources.

Implementation Date: December 31, 2021

Responsible Party: Alex Campoe, 813-974-1796