STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2022-133
February 2022

VALENCIA COLLEGE

ELLUCIAN BANNER® ENTERPRISE RESOURCE PLANNING SYSTEM

Sherrill F. Norman, CPA
Auditor General

Board of Trustees and President

During the period April 2020 through April 2021, Dr. Sanford C. Shugart served as President of the Valencia College and the following individuals served as Members of the Board of Trustees:

	County
Tracey Stockwell, Chair	Orange
Daisy Lopez-Cid, Vice Chair	Osceola
Dr. Bruce A. Carlson	Osceola
John F. Davis	Orange
Angel de la Portilla from 1-27-21	Orange
Maria C. Grulich	Osceola
Guillermo Hansen	Osceola
Michael A. Sasso	[a]
Beth Smith	Orange
Mai Swanson through 5-18-20[b]	Orange

[a] Confidential pursuant to Section 119.071(4), Florida Statutes.

[b] Trustee resigned 5-18-20, and Trustee position remained vacant through 1-26-21.

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

VALENCIA COLLEGE

Ellucian Banner® Enterprise Resource Planning System

SUMMARY

This operational audit of Valencia College (College) focused on selected information technology (IT) controls applicable to Valencia College Ellucian Banner® Enterprise Resource Planning System (Banner® ERP) system for maintaining and processing student account information and the infrastructure supporting the College Banner® ERP system. Our operational audit disclosed the following:

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

Finding 2: College IT security controls over user authentication, account management, mobile device management, vulnerability management, and logging and monitoring need improvement to ensure the confidentiality, integrity, and availability of College data and IT resources.

BACKGROUND

Valencia 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 to record, process, and report finance and human resources transactions and student information. 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

Effective application security management controls include resource owners identifying specific employees and authorizing the nature and extent to which those employees may access the resources where the owner has functional responsibility. Granting access to information technology (IT) resources based on a demonstrated need to view, change, or delete data and restricting individuals from performing incompatible functions or functions outside of their areas of responsibility is necessary to protect data and IT resources from unauthorized disclosure, modification, or destruction. In addition, documented periodic evaluations of access privileges associated with security groups help ensure that access privileges provided to each security group remain appropriate and necessary.

The Banner® ERP system forms are screens or pages that allow either data field modification, view, or both. Security within the Banner® ERP system student module controls user access to forms that relate to functions necessary for student administration, curriculum management, and student record maintenance and is based on assigning the forms to users directly or through user groups. Because of the COVID-19 pandemic, the College delayed evaluation of Banner ERP® system access privileges and, as of January 2021, the last evaluation of these privileges was in 2019. That evaluation included ensuring the appropriateness for groups assigned to users and, although some individual forms assigned to users through groups were evaluated for continued appropriateness, a comprehensive evaluation of all critical forms assigned to users through groups had not been performed.

Through inquiry with College personnel and examination of College records, we identified seven forms that allowed access to view or modify critical or confidential student-related information, including course information and student academic history, residency status, demographic and personally identifiable information (name, personal identifier, date of birth), placement test scores, and other course, graduation, and transfer data. In response to our request, College records were provided disclosing that 699 Banner® ERP system active user accounts were assigned modify access privileges to one or more of the seven forms as of January 2021.

Subsequent to our inquiry regarding the appropriateness of access privileges assigned and, in addition to the College-initiated evaluation of user group assignments within the student module in March 2021, the College's student data owner evaluated the appropriateness of the modify access privileges assigned to users for each of the seven forms. Our review of College records and College evaluations, as of May 2021, disclosed that the access privileges for one or more of the seven forms for 258 user accounts, including certain College employees[1] and certain University of Central Florida (UCF) employees,[2] were inappropriate or unnecessary. According to College management in June 2021, the identified inappropriate or unnecessary privileges had been or would be removed or changed to inquiry, as appropriate.

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

Recommendation: College management should enhance procedures to ensure that individuals are restricted from performing incompatible functions or functions outside their areas of responsibility. Such enhancements should include the performance of periodic comprehensive evaluations, on at least an annual basis, of access privileges granted to student information within the Banner® ERP system, including evaluating access privileges granted to critical forms, to verify that the privileges are necessary and appropriate for each user's assigned responsibilities.

[1] Employees with inappropriate or unnecessary access privileges included, for example, a student services advisor who no longer required that level of access when the advisor changed job duties; the Administrative Manager for the Criminal Justice Institute who had duty changes that no longer required update access to certain student record information; and a records specialist who no longer needed update access to student academic history information.

[2] The UCF and the College partnered to have a downtown campus with various programs, certificates, and training. While the College assigned certain UCF employees to user groups for enrollment, advising, and other student-related duties, the duties for certain UCF employees no longer required access to the student-related information.

Finding 2: Security Controls – User Authentication, Account Management, Mobile Device Management, Vulnerability Management, and Logging 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, account management, mobile device management, vulnerability management, and logging 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, account management, mobile device management, vulnerability management, and logging 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 College management improve IT security controls related to user authentication, account management, mobile device management, vulnerability management, and logging 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 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 January 2021 through October 2021 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 College IT controls to the Ellucian Banner Enterprise Resource Planning (Banner® ERP) system for maintaining and processing student account information and the Banner® ERP system supporting infrastructure during the period April 2020 through April 2021, 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.

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 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:

- Reviewed applicable laws, rules, 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.
- Evaluated 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 (servers), and the database management system (database); Banner® ERP system application, supporting server, and network device change management; and mobile device management.
- Evaluated the effectiveness of College logical access controls assigned to the College network, servers, and database supporting the Banner® ERP system, including the periodic evaluation of assigned accounts.
- Evaluated the effectiveness of logical controls assigned within the Banner® ERP system student module, including College procedures related to the periodic evaluation of assigned user access privileges.
- 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 selected scan reports, audit policies, logs, and documents to evaluate the adequacy of College vulnerability management controls related to the IT infrastructure supporting the Banner®

ERP system, including vulnerability assessment and remediation, maintenance, monitoring, and analysis of audit logs, secure server administration, and malware defense.

- Evaluated the appropriateness of controls for managing mobile devices (entity and non-entity owned cell phones and laptops) connected to the business network or used for storing confidential and sensitive data, including adequate policies and procedures defining the use and control of mobile devices and tools for the enforcement of appropriate security controls.
- Examined and evaluated the appropriateness of all accounts assigned administrator access privileges within the four default network administrator system groups for the College root domain as of January 15, 2021.
- Examined and evaluated, as of January 15, 2021, the 140 domain accounts not required to have a password change.
- Examined and evaluated the appropriateness of access privileges granted on the 10 servers supporting the Banner® ERP system. Specifically, as of January 15, 2021, we examined:
    - The 59 accounts assigned to one or more of the 5 database servers supporting the Banner® ERP system
    - The 33 accounts assigned to one or more of the 5 application servers supporting the Banner® ERP system.
- Examined and evaluated, as of January 15, 2021, all accounts defined to the application and database servers supporting the Banner® ERP system not required to have a password change.
- Evaluated College procedures and reviewed reports related to the recording, documenting, and reporting of changes to confidential and critical student record information within the Banner® ERP system student module to determine the adequacy of College logging and monitoring controls related to student information.
- Evaluated College procedures related to Banner® ERP system 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.
- Examined selected database and server logs to determine the adequacy of College logging and monitoring controls designed for the infrastructure supporting the Banner® ERP system, including actions performed by privileged users.
- Examined and evaluated the appropriateness of access privileges, as of January 21, 2021, granted within the Banner® ERP system student module for the 699 accounts with access to one or more of the seven forms granting access to confidential or critical student record fields.
- Examined and evaluated the appropriateness of the 35 accounts assigned selected administrative access privileges, as of January 20, 2020, to the database supporting the Banner® ERP system.
- Examined and evaluated, as of January 20, 2021, all accounts defined to the database supporting the Banner® ERP system not required to have a password change.
- Examined and evaluated, as of January 20, 2021, the appropriateness of the 16 accounts with default passwords defined to the database supporting 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, CPA
Auditor General

MANAGEMENT'S RESPONSE

VALENCIACOLLEGE

February 14, 2022

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

Dear Ms. Norman:

Enclosed is Valencia College's response to the audit findings included in the 2021 Information Technology Operational Audit of the Valencia College Ellucian Banner Enterprise Resource Planning System by the State of Florida.

Sincerely,

Kathleen Plinske

Kathleen Plinske, Ed.D.
President

Valencia College
Post Office Box 3028
Orlando, FL 32802-3028
407 299 5000
valenciacollege.edu

Valencia College
Responses to Preliminary and Tentative Audit Findings of the 2021 Information Technology Operational Audit of the Valencia College Ellucian Banner Enterprise Resource Planning System
Conducted by the Auditor General's Office

Finding 1: Application Security Management

Recommendation: College management should enhance procedures to ensure that individuals are restricted from performing incompatible functions or functions outside their areas of responsibility. Such enhancements should include the performance of periodic comprehensive evaluations, on at least an annual basis, of access privileges granted to student information within the Banner® ERP system, including evaluating access privileges granted to critical forms, to verify that the privileges are necessary and appropriate for each user's assigned responsibilities.

Management's Response: The College agrees with the recommendations and will enhance procedures to ensure that access granted to student information within the Banner ERP system is necessary and appropriate for the business of supporting our students. We have improved the quality of the Banner and Oracle database security reports that are available to the functional staff. This will allow those responsible within each functional area to perform periodic comprehensive evaluations of staff's security access in Banner and the Oracle database. These reviews will be performed annually.

Finding 2: Security Controls – User Authentication, Account Management, Mobile Device Management, Vulnerability Management, and Logging and Monitoring

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

Management's Response: The College has reviewed the findings and will continue to evaluate and implement improvements to the IT security controls related to user authentication, account management, mobile device management, vulnerability management, and logging and monitoring to ensure the confidentiality, integrity, and availability of College data and IT resources.