STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2023-048
November 2022

FLORIDA GATEWAY COLLEGE

Ellucian Banner® Enterprise Resource Planning System

Sherrill F. Norman, CPA
Auditor General

Board of Trustees and President

During the period August 2021 through July 2022, Dr. Lawrence M. Barrett served as President of Florida Gateway College and the following individuals served as Members of the Board of Trustees:

	County
John D. Crawford, Chair	Baker
Carolyn Renae Allen, Vice Chair	Union
Robert C. Brannan III	Baker
Lindsey Lander	Gilchrist
Kathryn L. McInnis	Dixie
Suzanne M. Norris	Columbia
Dr. James Surrency	Gilchrist
Dr. Miguel Tepedino	Columbia
Vacant [a]	Columbia

[a] Position vacant during the entire period.

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) 412-2923.

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 GATEWAY COLLEGE

Ellucian Banner® Enterprise Resource Planning System

SUMMARY

This operational audit of Florida Gateway College (College) focused on selected information technology (IT) controls applicable to the Banner® Enterprise Resource Planning (Banner® ERP) system and included a follow-up on applicable findings noted in our report No. 2018-123 (Findings 1, 2, 3, and 5). Our audit disclosed the following:

Finding 1: College controls over application security management need improvement to ensure that access privileges to student and accounts receivable information granted within the Banner® ERP system are necessary and appropriate. A similar finding was noted in our report No. 2018-123.

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

BACKGROUND

Florida Gateway 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 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 employees 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.

Banner® ERP system forms are screens or pages that allow either data field modification, view, or both. Security within the Banner® ERP system student and accounts receivable modules is based on controlling users' access to forms that relate to functions necessary for student administration, curriculum

management, student record maintenance, and student accounts receivable information. We examined access privileges as of February 2022 for all active Banner® ERP system accounts assigned access to the 12 selected critical forms related to student record information and payment and charge information for student accounts and found that improvements in application security management were needed. Specifically, for 37 employees assigned access privileges to 1 or more of the 12 forms, we found that:

- 8 employees assigned access privileges to the course registration form had the ability to update student residency status, although the 8 employees did not have responsibilities for assessing tuition. 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 Florida College System institutions. While the 8 employees' responsibilities necessitated update access to some data fields within the course registration form, because the access privileges granted to a form allow the user access to all data fields and tabs within the form, the employees' access privileges also unnecessarily provided the ability to update student residency and impact student tuition assessments. In response to our inquiry, College management stated that, based on our inquiries, the ability to update the course registration form would no longer be necessary for the employees' responsibilities and the privileges had been removed as of August 2022 for the 8 employees.
- 1 other employee had the ability to update student academic and course registration information although the access was no longer necessary following the employee's transfer to a new position in October 2021. In response to our inquiry, College management removed the employee's access privileges as of April 2022.
- 2 of the 6 employees with update access privileges to one or more of four student accounts receivable screens had access privileges that were no longer necessary for their assigned responsibilities due to promotion or other changes in responsibilities. Subsequent to our inquiry, in May 2022 College management indicated that the unnecessary access privileges were removed.

Appropriately restricted access privileges help protect College data and IT resources from unauthorized modification, loss, or disclosure. A similar finding was noted in our report No. 2018-123.

Recommendation: College management should continue to ensure that the access privileges granted to student information and accounts receivable within the Banner® ERP system are necessary and appropriate for the employee's assigned responsibilities.

Finding 2: Security Controls – User Authentication and 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 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 three findings in the two areas needing improvement.

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

[1] Section 1009.21, Florida Statutes.

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

PRIOR AUDIT FOLLOW-UP

Except as discussed in Finding 1, the College had taken corrective actions for the applicable findings included in our report No. 2018-123.

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 information technology (IT) operational audit from March 2022 through July 2022 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 applicable to the Ellucian Banner® Enterprise Resource Planning (Banner® ERP) system for maintaining and processing financial and human resources information and the Banner® ERP system supporting infrastructure during the period August 2021 through July 2022. For those areas addressed by this audit, our audit objectives were to:

- Determine the effectiveness of selected significant 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.
- Determine whether management had taken corrective actions for applicable deficiencies disclosed in our report No. 2018-123 (Findings 1, 2, 3, and 5).
- 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 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, waste, abuse, or inefficiency.

In conducting this audit, we:

- Reviewed applicable laws, rules, College policies and 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); and Banner® ERP system application, supporting server, and network device change management.
- Evaluated the effectiveness of College logical access controls assigned to the College network, servers, and database supporting the Banner® ERP system and selected College firewall, including the periodic evaluation of assigned accounts.
- Evaluated the effectiveness of logical controls assigned within the Banner® ERP system student and accounts receivable modules, including College procedures related to the periodic evaluation of assigned user access privileges.
- Evaluated the controls over collections of payments for cosmetology services to determine whether duties were appropriately separated and promoted accurate revenue amounts in the Banner® ERP system accounts receivable module.
- 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 network settings and 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.
- Evaluated College procedures and examined selected scan reports and policies to evaluate the adequacy of College vulnerability management controls related to the Banner® ERP system supporting IT infrastructure, including vulnerability assessment and remediation, maintenance, monitoring, and analysis of audit logs and malware defense.

- Examined and evaluated the appropriateness of all accounts assigned administrator access privileges, as of March 10, 2022, within the four default network administrator system groups for the College root domain.
- Examined and evaluated the appropriateness of the eight accounts assigned administrator access privileges, as of May 16, 2022, for a selected College firewall.
- Examined and evaluated, as of March 11, 2022, the 99 root domain accounts not required to have a password change.
- 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.
- 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.
- From the 12 selected critical forms related to student record information and payment and charge information for student accounts, examined and evaluated the appropriateness of access privileges, as of February 28, 2022, granted within the Banner® ERP system student module for the 31 accounts with access to one or more of the 8 forms granting access to confidential or critical student record fields and within the accounts receivable module for the six accounts with access to one or more of the 4 forms granting access to critical payment and charge information for student accounts.
- Examined and evaluated the appropriateness of access privileges granted on the 3 servers supporting the Banner® ERP system. Specifically, as of March 10, 2022, we examined:
    - The 53 accounts assigned to the database server supporting the Banner® ERP system.
    - The 30 accounts assigned to the 2 application servers supporting the Banner® ERP system.
- Examined and evaluated the appropriateness of the 12 accounts assigned selected administrative access privileges, as of February 28, 2022, 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

FLORIDA GATEWAY COLLEGE

From the Office of the President

October 19, 2022

Ms. Sherill F. Norman, CPA
Auditor General of the State of Florida
Claude Denson Pepper Building, Suite G74
111 West Madison Street
Tallahassee, FL 32399-1450

Dear Ms. Norman:

The following is the response to the preliminary and tentative findings of your IT audit of Florida Gateway College.

Finding No. 1 **Application Security Management**

Recommendation: College management should continue to ensure that the access privileges granted to student information and accounts receivable within the Banner® ERP system are necessary and appropriate for the employee's assigned responsibilities.

Response: The College agrees with the recommendation.

The Executive Director of Information Technology will implement automated processes which will identify position changes among College personnel and notify management when a review of access privileges may be warranted.

In addition, the Director of Enrollment Services has implemented a procedure to enable auditing of registration activity performed outside of the Enrollment Services department, which will be reviewed on a monthly basis.

Finding No. 2 **Security Controls – User Authentication and Account Management**

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

Response: The College agrees with the recommendation and will implement procedures to improve the IT security controls related to user authentication and account management.

Sincerely,

Lawrence Barrett, President

Michelle Holloway, Vice President for Business Services