STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2022-199
June 2022

HILLSBOROUGH COMMUNITY COLLEGE

ELLUCIAN COLLEAGUE ENTERPRISE RESOURCE PLANNING SYSTEM

Sherrill F. Norman, CPA
Auditor General

Board of Trustees and President

During the period August 2020 through August 2021, Dr. Kenneth H. Atwater served as President of Hillsborough Community College and the following individuals served as Members of the Board of Trustees:

Brigadier General Arthur “Chip” Diehl III (Ret.), Chair from 6-19-21
Vice Chair through 6-18-21
Randall H. Reid, Chair through 6-18-21
Nancy Watkins from 12-23-20, Vice Chair from 6-19-21
Gregory Celestan from 12-24-20
Brian Lametto from 12-24-20
Aakash M. Patel from 6-19-21
Dipawali Shah through 12-23-20
Betty Viamontes through 12-23-20

The team leader was George W. Phillips, CISSP, 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

HILLSBOROUGH COMMUNITY COLLEGE

Ellucian Colleague Enterprise Resource Planning System

SUMMARY

This operational audit of Hillsborough Community College (College) focused on evaluating selected information technology (IT) controls applicable to the Ellucian Colleague Enterprise Resource Planning (Colleague ERP) system for maintaining and processing student account information and the infrastructure supporting the College Colleague ERP system. Our 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 Colleague ERP system are necessary and appropriate.

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

BACKGROUND

Hillsborough Community 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 five 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 Colleague Enterprise Resource Planning (Colleague 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 Colleague ERP system.

FINDINGS AND RECOMMENDATIONS

Finding 1: Application Security Management

Effective application security management controls include resource owners with functional responsibility identifying specific employees and authorizing the nature and extent to which those employees may access the resource. 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.

Security within the Colleague ERP system student module is based on controlling users' access to screens to view or modify system information related to student information such as academic records,

recruiting and admissions, demographics, and registration. Through inquiry with College personnel and examination of College records, we identified seven screens that allowed access to view or modify critical or confidential student related information, including residency status, final grades, address, academic holds, class registration, and test scores.

Our examination of the access privileges as of August 2021 for all 456 Colleague ERP system employee accounts assigned access to one or more of the seven screens disclosed that 11 employees could update certain screen information, including residency, grades, holds, registration, and test scores,[1] although such updates were not part of their assigned duties. Subsequent to our inquiry, College management indicated that, as of February 2022, the access privileges for the 11 employees had been removed or modified to more appropriately reflect the employees' assigned job duties.

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

Recommendation: College management should continue to ensure that access privileges granted to student information within the Colleague ERP system restrict employees from performing incompatible functions or functions outside their areas of responsibility.

Finding 2: Security Controls – User Authentication, Account Management, and Vulnerability 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, account management, and vulnerability 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 four findings in the three areas needing improvement.

Without appropriate security controls related to user authentication, account management, and vulnerability management, 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, and vulnerability management 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.

[1] Employees with inappropriate or unnecessary access privileges included, for example, a marketing and communications coordinator who could update student academic holds and test score information; a campus business assistant who could update student residency status, academic holds, and test score information; a facilities planner who could update test scores; and a staff assistant who could update students' final grades and class registrations.

We conducted this information technology (IT) operational audit from June 2021 through February 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 Hillsborough Community College (College) IT controls applicable to the Ellucian Colleague Enterprise Resource Planning (Colleague ERP) system for maintaining and processing student account information and the Colleague ERP system supporting infrastructure during the period August 2020 through August 2021, and selected actions subsequent thereto. 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.
- 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 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 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, College procedures, and other guidelines; interviewed College personnel; and examined College records to obtain an understanding of College operations related to the Colleague ERP system and to determine 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 College IT processes for the Colleague 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); Colleague 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 Colleague ERP system, including the periodic evaluation of assigned accounts.
- Evaluated the effectiveness of logical controls assigned within the Colleague ERP system student module, including College procedures related to the periodic evaluation of assigned user access privileges.
- Examined selected security settings related to the Colleague 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 and evaluated the adequacy of College vulnerability management controls related to the IT infrastructure supporting the Colleague 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 the adequacy of the 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, as of June 7, 2021, within the four default network administrator system groups for the College root domain.
- Examined and evaluated the appropriateness of all unique accounts assigned administrator access privileges, as of June 7, 2021, for the 23 member servers supporting the Colleague ERP system.
- Examined and evaluated, as of June 7, 2021, the 36 root domain user accounts not required to have a password change.
- Examined and evaluated the appropriateness of access privileges granted on the database supporting the Colleague ERP system. Specifically, as of June 7, 2021, we examined:
    - The 18 accounts with the ability to connect to both the database service and database with administrative privileges.
    - The 22 accounts with the ability to connect to the database with administrative privileges.
- Examined and evaluated, as of June 7, 2021, the 12 accounts defined to the database supporting the Colleague 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 Colleague

ERP system student module to determine the adequacy of College logging and monitoring controls related to student information.

- Evaluated College procedures related to Colleague ERP system patches, upgrades, and data fixes and changes to supporting infrastructure, including system software and selected firewall, and determined whether the procedures required modifications to be appropriately authorized, tested, and approved.
- 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 Colleague ERP system, including actions performed by privileged users.
- Examined and evaluated the appropriateness of access privileges, as of August 31, 2021, granted within the Colleague ERP system student module for the 456 accounts with access to one or more of the seven screens 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

Office of the President | Dr. Ken Atwater

May 26, 2022

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

Dear Ms. Norman,
We are pleased to respond to the preliminary and tentative audit findings and recommendations concerning the information technology operational audit of Hillsborough Community College's ERP system. Our responses to the findings are listed below:

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

Recommendation: College management should continue to ensure that access privileges granted to student information within the Colleague ERP system restrict employees from performing incompatible functions or functions outside their areas of responsibility.

Response: College management agrees with the recommendation and will continue to improve the current processes to ensure that access privileges granted to student information within the Colleague ERP system restrict employees from performing incompatible functions or functions outside their areas of responsibility.

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

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

Response: College management agrees with the recommendation and has taken corrective actions to improve IT security controls over account management, and vulnerability management to ensure the confidentiality, integrity, and availability of college data and IT resources.

If you have any questions regarding this information, please feel free to contact me at 813.253.7050.

Sincerely

Dr. Ken Atwater
President,
Hillsborough Community College

Hillsborough Community College
39 Columbia Drive, Tampa, FL 33606-3584 | 813.253.7050 | 813.253.7183 fax | hccfl.edu