STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2024-003
August 2023

BROWARD COLLEGE

Workday® Enterprise Cloud Applications

Sherrill F. Norman, CPA
Auditor General

Board of Trustees and President

During the period November 2021 through October 2022, Gregory Adam Haile, Esq. served as President of Broward College and the following individuals served as Members of the Board of Trustees:

Gloria M. Fernandez, Chair through 8-9-22
Zachariah "Reggie" P. Zachariah Jr., Vice Chair through 8-9-22, Chair from 8-10-22
Akhil K. Agrawal, Vice Chair from 8-10-22
Matthew Caldwell J.D. through 8-31-22 [a]

[a] Trustee position vacant from 9-1-22, through 10-31-22.

Note: One Trustee position was vacant for the entire period.

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

BROWARD COLLEGE

Workday® Enterprise Cloud Applications

SUMMARY

This operational audit of Broward College (College) focused on evaluating selected information technology (IT) controls applicable to the Workday® Enterprise Cloud Applications and the College's IT infrastructure, and included a follow-up on the findings included in our report No. 2020-015. Our audit disclosed the following:

Finding 1: College security awareness training needs improvement to reduce the risk for College data to be compromised.

Finding 2: Certain College IT security controls related to user authentication, account management, configuration management, and vulnerability management need improvement to ensure the confidentiality, integrity, and availability of College data and IT resources. A similar finding related to account management was noted in our report No. 2020-015.

BACKGROUND

Broward 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 Workday® Enterprise Cloud Applications (Workday®) to record, process, and report finance and human resources transactions. Workday, Inc. hosts the College's subscription to Workday® using Software as a Service and maintains and manages the supporting infrastructure. The College uses the Central Integrated Database (CID) student legacy system to record student information. The College maintains and manages the network domains supporting access to Workday®, CID, and College information technology infrastructure and the servers and database supporting CID.

FINDINGS AND RECOMMENDATIONS

Finding 1: Security Awareness Training

A comprehensive security awareness training program instructing all employees on the importance of preserving the confidentiality, integrity, and availability of data and information technology (IT) resources entrusted to them is a foundational control for security vigilance and a college's prevention and mitigation of cybersecurity risks. An effective security awareness program includes identification of the specific knowledge, skills, and abilities needed to support College security and educates all employees about data handling best practices and how to interact with data and IT resources in a secure manner.

According to College personnel, security awareness training was mandatory and provided by third-party software within 30 days of hire for new employees and annually for other employees. However, our examination of College records disclosed that the training did not educate employees about data handling best practices specific to College controls. In addition, although we requested, College records were not provided to demonstrate that employees had completed the training during the period November 2021 through October 2022. In response to our inquiry, College management indicated that the software could not be customized for training on best practices specific to College controls and did not have the capability to monitor and track the training.

Effective security awareness training programs include data handling best practices and instructions to understand causes of unintentional data exposure and require training with metrics to ensure completion by all employees. The lack of a comprehensive security awareness training program increases the risk that employees may compromise the confidentiality, availability, and integrity of College data and IT resources.

Recommendation: To reduce cybersecurity risks, College management should establish a comprehensive security awareness training program to ensure and document that employees are aware of their responsibilities and the importance of securing College data and IT resources and complete the required training.

Finding 2: Security Controls – User Authentication, Account Management, Configuration 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, configuration 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 five findings in the four areas needing improvement. A similar finding related to account management was noted in our report No. 2020-015.

Without appropriate security controls related to user authentication, account management, configuration 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, configuration management, and vulnerability management to ensure the confidentiality, integrity, and availability of College data and IT resources.

PRIOR AUDIT FOLLOW-UP

As discussed in Finding 2, the College had not taken corrective action for the finding included in our report No. 2020-015.

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 August 2022 through May 2023 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 Workday® Enterprise Cloud Applications (Workday®) and College IT infrastructure during the period November 2021 through October 2022, 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 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 had corrected, or was in the process of correcting, deficiencies disclosed in our report No. 2020-015.
- 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 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, and other guidelines to obtain an understanding of College organizational structure and regulatory requirements; reviewed College procedures, interviewed College personnel, and examined College records to obtain an understanding of College operations related to Workday® and IT infrastructure 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 Workday® and College IT infrastructure, including authentication, backup and recovery, configuration of systems, logical controls, and inventory and vulnerability management.
- Examined selected security settings related to College network infrastructure, externally facing applications, remote access systems, and other critical servers and devices to determine whether authentication controls were configured and enforced in accordance with IT best practices, including the use of multi-factor authentication.
- Evaluated the effectiveness of College logical access controls assigned to the College network, selected network devices, and servers supporting the Central Integrated Database student legacy system (CID), including the periodic evaluation of assigned accounts.
- Examined and evaluated the appropriateness of all accounts assigned administrator access privileges, as of August 25, 2022, within three of the four default network administrator system groups for the College root domain.
- Examined and evaluated, as of August 25, 2022, the 70 root domain user accounts not required to have a password change.
- Examined and evaluated the appropriateness of all accounts assigned administrator access privileges, as of September 8, 2022, for the 14 College high-risk network devices.
- Examined and evaluated the appropriateness of all accounts assigned selected administrative access privileges as of September 9, 2022. Specifically, we examined and evaluated:
    - 28 accounts on 1 one critical network member server for CID.
    - 33 accounts on 1 or more of the 3 servers supporting CID.
- Examined and evaluated selected College patch management controls for operating systems and network devices to ensure secure configurations are maintained. Specifically, we examined and evaluated:
    - 110 network servers as of December 2, 2022.
    - The 14 high-risk network devices as of January 19, 2023.
- Evaluated College procedures and examined selected backup testing reports to determine the adequacy of the College data recovery procedures to restore College IT assets to a pre-incident trusted state.
- Evaluated the effectiveness of College configuration management controls, including establishing and maintaining secure configurations; disabling insecure protocols; implementing firewalls or

port filtering to protect network resources; and timely applying software updates and managing device end-of-life.

- Evaluated College procedures and examined selected records to determine the adequacy of College procedures for maintaining a software asset inventory and ensuring only authorized software is installed on the network.
- Evaluated the effectiveness of College security awareness training.
- Evaluated College procedures and examined selected scan reports and policies to evaluate the adequacy of College vulnerability management controls related to the IT infrastructure, including vulnerability assessment and remediation, malicious software identification, and malware defense.
- 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

BROWARD COLLEGE
www.broward.edu

INFORMATION TECHNOLOGY
Cypress Creek Administrative Center
6400 N.W. 6th Way, Fort Lauderdale, FL 33309
Phone 954-201-7520/Fax 954-201-7054

July 28, 2023

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

Dear Ms. Norman,

The purpose of this letter is to respond to the preliminary and tentative audit finding and recommendation resulting from the Information Technology operational audit of Broward College, Workday Enterprise Cloud Applications.

Pursuant to Section 11.45(4)(d), Florida Statutes, this is our written statement of explanation concerning the finding, including our actual and proposed corrective action. Below is a response for each finding:

SUMMARY:
Finding 1: College security awareness training needs improvement to reduce the risk for College data to be compromised.

Finding 2: Certain College IT security controls related to user authentication, account management, configuration management, and vulnerability management need improvement to ensure the confidentiality, integrity, and availability of College data and IT resources. A similar finding related to account management was noted in our report No. 2020-015.

CORRECTIVE ACTIONS:
Finding 1: Security Awareness Training.
We will improve our ability to monitor, track, and report on security awareness training to provide the evidence required to reflect the existence of an effective training program for new and existing employees.

Finding 2: IT security controls related to user authentication, account management, and vulnerability management.
We will continue to improve our security controls.

We appreciate the opportunity to respond to these findings.

Sincerely,

Raj Mettai
Interim Vice President, Information Technology

copy: Heidi Burns, Audit Manager, Information Technology Audits
George W. Phillips, Lead Senior IT Auditor
Lacey Hofmeyer, General Counsel & VP, Public Policy & Government Affairs
Gregory Haile, President
Jeffrey Nasse, College Provost & Senior Vice President for Academic Affairs
Rabia Azhar, Vice President, Procurement and Chief Financial Officer