STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2020-015
August 2019

BROWARD COLLEGE

Workday® Enterprise Cloud Applications

Sherrill F. Norman, CPA
Auditor General

Board of Trustees and President

During the period October 2018 through January 2019, Gregory Haile, Esq., served as President of Broward College and the following individuals served as Members of the Board of Trustees:

Gloria M. Fernandez, Chair
David R. Maymon, Vice Chair
Matthew Caldwell
Dr. Rajendra P. Gupta through 10-5-18[a]
Edward Michael Rump

[a] Position vacant 10-6-18 through 1-31-19.

The team leader was Joseph D. Garcia, and the audit was supervised by Heidi G. 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 College information technology (IT) controls applicable to Workday® Enterprise Cloud Applications (Workday®), including the contractual relationship with Workday, Inc. as the provider for the College's Workday® Software as a Service subscription. As summarized below, our audit disclosed an area in which improvements in College controls and operational processes are needed. Our audit disclosed the following:

Finding 1: College controls related to network account management need improvement.

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 operations and administration of the College.

The College operates a data center located within a hosted facility, including servers, storage, networking, and security equipment that support the College's legacy Student Information System and critical operations and services across its campuses and remote centers. The College uses Workday® Enterprise Cloud Applications (Workday®) for the recording, processing, and reporting of finance and human resource transactions. The College executed a Master Subscription Agreement (MSA) with Workday, Inc. on September 28, 2012, for the subscription to Workday® using Software as a Service (SaaS). Under the terms of the MSA, Workday, Inc. hosts Workday® applications and maintains and manages the supporting information technology (IT) infrastructure.

FINDINGS AND RECOMMENDATIONS

Finding 1: Network Account Management

Effective management of network accounts is enhanced through controls that ensure that access granted to privileged accounts, including system and special purpose accounts (accounts defined for a specific service or application and not assigned to one specific user) and groups, is based on the performance of least functionality and disabled when no longer needed. Additionally, periodic access reviews are necessary to ensure that only authorized accounts have access and that the access provided to each account remains appropriate and necessary.

On April 1, 2017, the College contracted with Modcomp, Inc. dba CSPi Technology Solutions (CSPi) for managed services, including monitoring and supporting the College's Active Directory services for its

network, with an estimated termination date of June 30, 2020. The contract terms for CSPi's services include the configuration of Active Directory and optimization of the network through application of security best practices. During the contract period, the College has responsibility for notifying CSPi of change management activities related to the network, including service account changes such as naming, deleting, or changing privileges of accounts used in connection with devices covered under the contract.

Our review of all accounts granted the highest privileges within the College's Active Directory structure as of October 19, 2018, disclosed that 12 employee user accounts, 70 system and special purpose accounts, and 21 CSPi and other contractor accounts had administrative access privileges allowing full control over the College's network root domain. Allowing excessive numbers of individuals and accounts the ability to maintain administrative control of the network domain instead of delegating authority for such activities as managing Active Directory, creating or modifying user accounts, or supporting servers and workstations is unnecessary and contrary to best practices of limiting administrative access by least privilege principles wherein the minimum amount of access necessary is granted to an individual or account to accomplish assigned responsibilities. In addition, the College had not performed periodic reviews of domain access privileges since an internal review was performed by management in July 2016 and an external review was performed by CSPi during the initial phase of the contract in 2017.

In response to our audit inquiry, College management stated that 33 system and special purpose accounts and 2 contractor accounts would be disabled or removed and that additional accounts would be further evaluated. College management also indicated that the College had not subsequently performed a periodic review of the accounts because of significant changes in the College's department teams tasked with the review responsibilities and that the College intends to implement processes, including review procedures, consultation with CSPi, and use of access management software, to better secure and manage the privileges assigned to accounts on the network.

Appropriately restricted access privileges help protect data and IT resources from unauthorized modification, loss, or disclosure. Periodic reviews of network accounts and associated access privileges increase management's assurance that accounts continue to be appropriate and necessary.

Recommendation: We recommend that College management improve network account management by implementing security practices, including review procedures, to ensure that access privileges are assigned based on the need for least privilege and are disabled when no longer appropriate or necessary.

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 October 2018 through April 2019 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 IT controls applicable to Workday®, including the contractual relationship with Workday, Inc. as the provider for the SaaS subscription during the period October 2018 through January 2019, and selected actions subsequent thereto. The overall objectives of the audit 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; the safeguarding of IT resources; and the effectiveness and efficiency of IT operations.
- 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 and controls included within the scope of the audit, deficiencies in management's internal controls; 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 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:

- Interviewed College staff and reviewed documentation applicable to College and Workday, Inc. operations to obtain an understanding of:
    - The delineation of responsibilities between the College and Workday, Inc. for the security, administration, support, and maintenance of Workday® and the supporting IT infrastructure, and the applicable contractual provisions.

  - o IT infrastructure, including the hardware, operating systems, and database management system, as they relate to the support of the College's Workday® SaaS subscription.
  - o Workday® controls that support the College's critical finance and human resources business processes.
- Evaluated the adequacy of College security management controls for ensuring the sufficiency of activities performed by Workday, Inc. related to data management and security.
- Evaluated the adequacy of College security management controls for ensuring the sufficiency of Workday, Inc. controls related to restricting administrative access privileges to the IT infrastructure supporting Workday®.
- Evaluated the adequacy of College security management controls for ensuring the sufficiency of Workday, Inc. controls related to appropriateness of selected authentication controls for the IT infrastructure supporting Workday®.
- Evaluated the adequacy of College security management controls for ensuring the sufficiency of Workday, Inc. logging and monitoring controls over privileged administrator actions for the servers and database that support Workday®.
- Evaluated the effectiveness of selected logical access controls for restricting administrative access privileges to the College's network domain.
- Evaluated the adequacy of the College's security management controls related to user authorization, periodic review of access, and identification of sensitive transactions for Workday®.
- Evaluated the adequacy of the College's system documentation relating to Workday® to promote efficient and effective operations.
- Evaluated the adequacy of the College's logging and monitoring controls over changes to the security and configuration of Workday®, including changes to user access, security group permissions, and business process rules.
- Evaluated the adequacy of the College's controls related to security group and business process rule creation, assignment, and ongoing maintenance.
- Evaluated the adequacy of the College's controls over the security administration function for Workday®.
- Evaluated the appropriateness of selected authentication controls used to protect IT resources and College data for Workday®.
- Examined and evaluated the appropriateness of administrative privileges for the College's network domain as of October 19, 2018.
- Examined and evaluated access granted to 11 critical Workday® business processes to determine whether the processes enforce an appropriate separation of duties.
- Examined and evaluated access granted to the Workday® security group to determine whether security administrator functions were appropriately granted to College personnel.
- 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

August 13, 2019

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,

Enclosed is the response 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.

SUMMARY:
Finding 1: College controls related to network account management need improvement.

CORRECTIVE ACTIONS:
Finding 1: Network Account Management

We have taken actions, as appropriate, to address accounts with administrative access privileges, and will continue to use best practices to more effectively manage and review privileged accounts.

We will review privileged accounts quarterly, with documented evidence, to make sure that we remain in compliance with current requirements.

Sincerely,

Tony Casciotta
Vice President, Information Technology

Enclosure

copy: Heidi Burns, Audit Manager, Information Technology Audits
Joseph Garcia, Senior Auditor
Lacey Hofmeyer, General Counsel & VP, Public Policy & Government Affairs
Gregory Haile, President