STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2023-067
December 2022

PENSACOLA STATE COLLEGE

Workday® Enterprise Cloud Applications

Sherrill F. Norman, CPA
Auditor General

Board of Trustees and President

During the period September 2021 through August 2022, Dr. Charles Edward Meadows served as President of Pensacola State College and the following individuals served as Members of the Board of Trustees:

	County
Marjorie T. Moore, Chair	Escambia
Harold Edward Moore, Vice Chair	Escambia
Patrick R. Dawson	Santa Rosa
Julian MacQueen	Santa Rosa
Carol H. Carlan	Escambia
Kevin Robert Lacz	Santa Rosa
Dr. Troy Tippett	Escambia

Note: Two trustee positions were vacant for 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) 412-2926.

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

PENSACOLA STATE COLLEGE

Workday® Enterprise Resource Planning System

SUMMARY

This operational audit of Pensacola State College (College) focused on evaluating selected information technology (IT) controls applicable to the Workday® Enterprise Cloud Applications (Workday®) for maintaining and processing financial, human resources, and student information and the infrastructure supporting Workday®. Our audit disclosed the following:

Finding 1: College controls over application configuration management need improvement to ensure that changes to business processes and security groups are appropriately authorized, tested, and approved and documented for routine monitoring.

Finding 2: College controls over periodic access reviews need improvement to ensure that access privileges granted within Workday® are necessary and appropriate.

Finding 3: College IT security controls over account management, vulnerability management, and configuration management needed improvement to ensure the confidentiality, integrity, and availability of College data and IT resources.

BACKGROUND

Pensacola State 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 Workday® Enterprise Cloud Applications (Workday®) to record, process, and report financial, human resources, and student information. The College executed a master subscription agreement, effective January 23, 2019, with Workday, Inc. to host the Workday® applications. In addition, the College maintains and manages the network domain supporting access to Workday®.

FINDINGS AND RECOMMENDATIONS

Finding 1: Application Configuration Management

Effective application configuration management provides a framework for managing changes to application functionality and security and for monitoring such changes to ensure the application is configured as intended. Managing changes to business processes and security groups to ensure continued data and process integrity requires proper authorization, testing, approval, and tracking of all changes.

The College implemented the Workday® finance and human resources applications in January 2021 and the Workday® student application in March 2022. Workday® security is segmented by application-delivered functional areas and further defined by domains, such as reports and tasks, and business processes within functional areas. Workday® business processes are a set of configurable steps performed within an automated workflow to complete transaction related changes to data and define each Workday® application's functionality.[1] An individual user navigates and accesses reports and tasks and participates in business process transactions within functional areas through assignment to a security group. Security groups define a specific set of responsibilities and permissions and determine the information that can be viewed and the tasks and transactions that can be initiated, completed, and approved.[2] Workday, Inc. maintains the delivered business processes for each Workday® application.

The College may customize the configuration of selected business processes by adding or deleting steps within the business process, changing the action performed within steps of a process, or changing the security group(s) that have the ability to perform each step. Security groups are customized through assigning users to groups and associating domain and business process security policies with each group. Domain security policies are modify or view privileges granted to each item within the domain and business process security policies are applied to the business processes. The business process security policies indicate the access granted for process steps to, for example, initiate, correct, reassign, rescind, approve, or view a process or part therein.

Our inquiries of College personnel regarding configuration management procedures for the Workday® applications disclosed that, although certain personnel had been granted the ability to modify business processes and security groups within Workday®, College management had not established procedures for authorizing, testing (where applicable), and approving changes to the business processes and security groups prior to implementation or for documenting the changes made. In addition, although reports detailing changes made to business processes and security groups within a given time period were available in Workday®, because College management was not aware of these reports, changes made to the business processes or security groups were not monitored to ensure that they had been authorized.

Changes to business processes and security groups impact the processing of transactions and overall security for the Workday® applications. Effective application configuration controls, including authorizing, testing (where applicable), and approving changes and documenting the changes made, reduce the risk that erroneous or unauthorized changes may be implemented or that authorized changes may not operate as intended.

Recommendation: We recommend that College management establish procedures to ensure that all business process and security group changes are appropriately authorized, tested, and approved prior to implementation and that documentation supporting the changes is maintained.

[1] Hiring an employee is a key business process within the Workday® human resources (HR) application.

[2] A security group may be created as role-based security and assigned based on a user's role or responsibility within the College. For example, the HR Partner role can initiate employment transactions such as hire, request one-time payment, or promotion and can view employment data, such as job details, personal information and compensation.

In addition, management should routinely monitor the changes to ensure that only authorized changes were made.

Finding 2: Periodic Access Review

Effective IT access controls include assigning employees access to IT resources based on a demonstrated need to view, change, or delete data along with a periodic review of the assigned employee access privileges. Periodic reviews of access privileges are necessary to ensure that employees can access only those IT resources that are necessary to perform their assigned job duties and that the assigned access privileges enforce an appropriate separation of incompatible duties.

In response to our inquiry, College personnel indicated that, as of October 2022, College management had not established or performed procedures for reviewing access privileges granted within Workday® to ensure that users and their associated security groups were appropriate and that access privileges associated with security groups remained appropriate. According to College personnel, Workday® could not generate reports necessary for reviewing access privileges. Subsequent to our inquiries, in June 2022 programming staff began developing reports for use in annual review procedures and, in November 2022, indicated that the reports had been submitted for management review.

Periodic reviews of security groups and associated access privileges increase management's assurance that user access continues to be appropriate and reduce the risk that unauthorized disclosure, modification, or destruction of College IT resources and data may occur.

Recommendation: We recommend that College management establish procedures for the periodic review of user access privileges. Such procedures should include use of reports identifying users and their associated security groups and access privileges to determine whether the privileges continue to be appropriate.

Finding 3: Security Controls –Account Management, Vulnerability Management, and Configuration 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 account management, vulnerability management, and configuration 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 areas needing improvement.

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

We conducted this information technology (IT) operational audit from April 2022 through November 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 controls applicable to the Workday® Enterprise Cloud Applications (Workday®) for maintaining and processing financial, human resources, and student information and the Workday® supporting infrastructure during the period September 2021 through August 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 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 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 the College infrastructure, including authentication, logical controls, vulnerability management, logging and monitoring, and configuration management.
- Examined the master subscription agreement between the College and Workday, Inc., effective January 23, 2019; Service Organization Controls 1 Report for the period April 1, 2021, to September 30, 2021; and Service Organization Controls 2 Report for the period October 1, 2020, to September 30, 2021, to determine the sufficiency of the College's assurance related to Workday, Inc.'s security and data management, logical, authentication, and logging and monitoring controls for the IT infrastructure supporting Workday® and disaster recovery planning controls.
- Evaluated the effectiveness of College logical access controls assigned to the College network and selected network devices, including the periodic evaluation of assigned accounts.
- Evaluated the effectiveness of security management controls for Workday®, including College procedures related to the periodic evaluation of assigned user access privileges.
- Evaluated College procedures and examined selected College records to determine the adequacy of logging and monitoring controls over changes to the security and configuration of Workday®, including changes to security groups and business processes.
- Evaluated College procedures and examined selected College records to determine the effectiveness of logging and monitoring user activity for critical finance and human resources transactions.
- Evaluated the membership assigned to the security administrator security group to determine the adequacy of College controls over the security administration function for Workday®.
- Evaluated selected security settings related to Workday® and the supporting College network infrastructure to determine whether authentication controls were configured and enforced in accordance with IT best practices.
- Evaluated College procedures and examined selected scan reports and policies to evaluate the adequacy of College vulnerability management controls related to the infrastructure supporting Workday®, including vulnerability assessment and remediation, malicious software identification, and malware defense.
- Examined and evaluated the appropriateness of all accounts assigned administrator access privileges, as of March 28, 2022, within the four default network administrator system groups for the College root domain.
- Evaluated the effectiveness of College configuration management controls, including timely applying software updates and managing device end-of-life.

- Examined and evaluated College patch management controls for all of the 351 higher risk network devices as of April 21, 2022, to ensure secure configurations are maintained.
- Examined network logging settings and related College reports to determine the adequacy of College logging and monitoring controls designed for the network infrastructure supporting Workday®.
- 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

Office of the President

Pensacola State College
1000 College Boulevard
Pensacola, FL 32504-8998
850-484-1700
Fax 850-484-1840
www.pensacolastate.edu

PENSACOLA STATE COLLEGE

December 12, 2022

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

Dear Ms. Norman:

Let me express our sincere appreciation for the professional manner in which your staff conducted the audit. Following are the College's responses to the preliminary and tentative findings to be included in the operational audit report.

Finding No. 1: Application Configuration Management

Recommendation: We recommend that College management establish procedures to ensure that all business process and security group changes are appropriately authorized, tested, and approved prior to implementation and that documentation supporting the changes is maintained. In addition, management should routinely monitor the changes to ensure that only authorized changes were made.

Response: The College has developed and implemented Security Request Frameworks in Workday to address configuration management and approvals. All Workday configuration changes must be made via this dynamic questionnaire that routes for multiple approvals based on the type of configuration change requested. The request, review, and approval for changes are documented within the security request frameworks. Administrative review will happen at least annually.

Finding No. 2: Periodic Access Review

Recommendation: We recommend that College management establish procedures for the periodic review of user access privileges. Such procedures should include the use of reports identifying users and their associated security groups and access privileges to determine whether the privileges continue to be appropriate.

Response: The College has currently established procedures to conduct a biennial review of access privileges, security group composition, report, and data access. The College has plans to develop reports for supervisor review and approval of employee access.

Finding No. 3: Security Controls – Account Management, Vulnerability Management, and Configuration Management

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

Response: The College will review and will improve IT security controls related to account management, vulnerability management, and configuration management.

Should you have any questions or concerns, please feel free to call me.

Sincerely,

Edward Meadows
President