STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2025-062
December 2024

# UNIVERSITY OF CENTRAL FLORIDA

## Workday Enterprise Cloud Applications

Sherrill F. Norman, CPA
Auditor General

## Board of Trustees and President

During the period June 2023 through May 2024, Dr. Alexander Cartwright served as President of the University of Central Florida and the following individuals served as Members of the Board of Trustees:

| | |
|---|---|
| Alex Martins, Chair | Joseph D. Conte |
| Harold Mills, Vice Chair through 5-13-24 [a] | Danny Gaekwad |
| Michael Okaty, Vice Chair from 5-17-24 [a] | Brandon Greenaway through 5-5-24 [b] |
| Tiffany Altizer | Dr. Stephen King [c] |
| Rick Cardenas | Bryce Lister from 5-6-24 [b] |
| Bill Christy | Caryl McAlpin |
| Jeff Condello | John Miklos |

[a] Vice Chair position vacant through 5-16-24.
[b] Student Body President.
[c] Faculty Senate Chair.

The team leader was George W. Phillips, CISA, CISSP, 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**

# UNIVERSITY OF CENTRAL FLORIDA

## Workday Enterprise Cloud Applications

## SUMMARY

This operational audit of the University of Central Florida (University) focused on selected information technology (IT) controls applicable to the Workday Enterprise Cloud Applications and the University's IT infrastructure. Our audit disclosed the following:

**Finding 1:** University controls over application security management need improvement to ensure that changes to business processes and security groups are appropriately authorized and approved, and access privileges granted within Workday are necessary and appropriate.

**Finding 2:** University security awareness training needs improvement to reduce the risk of compromising University data and IT resources.

**Finding 3:** Certain University IT security controls related to account management and configuration management need improvement to ensure the confidentiality, integrity, and availability of University data and IT resources.

## BACKGROUND

The University of Central Florida (University) is part of the State university system of public universities, which is under the general direction and control of the Florida Board of Governors (BOG). The University is directly governed by a Board of Trustees (Trustees) consisting of 13 members. The Governor appoints 6 citizen members and the BOG appoints 5 citizen members. These members are confirmed by the Florida Senate and serve staggered 5-year terms. The Faculty Senate Chair and Student Body President are also members. The BOG establishes the powers and duties of the Trustees. The Trustees are responsible for setting University policies, which provide governance in accordance with State law and BOG Regulations. The University President is selected by the Trustees and confirmed by the BOG. The University President serves as the Executive Officer and the Corporate Secretary of the Trustees and is responsible for administering the policies prescribed by the Trustees for the University.

The University uses the Workday Enterprise Cloud Applications (Workday) to record, process, and report finance and human resources transactions. Workday, Inc. hosts the University's subscription to Workday using Software as a Service and maintains and manages the supporting infrastructure. The University maintains and manages the network domain supporting access to Workday and University IT infrastructure.

## FINDINGS AND RECOMMENDATIONS

### Finding 1: Application Security Management

Effective application security management provides a framework for managing risk, developing policies, and monitoring the adequacy of application-related controls. As part of application security management,

managing changes to application functionality and security, along with appropriate monitoring of those changes, ensures the application is configured as intended. In addition, periodic reviews of access privileges associated with security roles help ensure that access provided to each security role remains appropriate and necessary. Periodic reviews of access privileges are also necessary to ensure that employees can access only those information technology (IT) resources that are necessary to perform their assigned job duties and that the assigned access privileges enforce an appropriate separation of incompatible duties.

The University implemented Workday in July 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.[1] 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. 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 University may customize the configuration of selected business processes by adding or deleting steps within a 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. As a Workday, Inc. customer, the University is responsible for controlling the access rights and authorization limits necessary for each end user to accomplish job responsibilities and should review the security accesses and authorization limits on a periodic basis and monitor all user access and authorization limits.

As part of our audit, we made inquiries of University personnel and examined University records supporting changes to business processes and security groups and reviews of access privileges within Workday. Based on our procedures, we found that improvements were needed for managing these changes and reviewing the access privileges. Specifically, as of September 2024:

- All changes made to business processes and security roles were automatically logged within Workday. According to the Workday Enterprise Systems (WES) team members granted the ability to modify business processes and security groups within Workday, procedures were established for manually recording authorization and approval for changes prior to implementation; however, the change logs were not periodically reviewed to ensure that all changes had been authorized and approved. In response to our inquiry, University management indicated that because WES team members hold positions of trust, they adhere to the procedures

[1] For example, 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 University. 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.

over documenting changes. Notwithstanding, management indicated that periodic reviews of the documented changes would be implemented.

- Although a review of security administration access privileges granted to the Workday implementation team had been performed in May and August 2023 upon the University transitioning to a support team, University management had not established or performed procedures for reviewing access privileges granted within Workday to ensure that all users and their associated security groups, along with the access privileges associated with the security groups, were appropriate. In response to our inquiry, University management indicated that a comprehensive process is being designed to annually evaluate access privileges, including report design and the development and determination of responsible reviewers and approvers.

Changes to business processes and security groups impact the processing of transactions and overall security for the Workday applications. Monitoring changes to business processes and security groups to ensure proper authorization and approval reduces the risk that erroneous or unauthorized changes may be implemented and that authorized changes may not operate as intended. Additionally, 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 University IT resources and data may occur.

**Recommendation: We recommend that University management establish procedures to monitor business process and security group changes so that all changes are appropriately authorized and approved. In addition, management should establish procedures for the periodic review of user Workday 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 2: 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 IT resources entrusted to them is a foundational control for security vigilance and preventing and mitigating cybersecurity risks. An effective security awareness program includes identification of the specific knowledge, skills, and abilities needed to support University security and educates all employees about how to interact with data and IT resources in a secure manner.

As part of our audit, we examined University procedures and related records supporting annual employee security awareness and skills training. We found that the Information Security Division within the Central Information Technology Department provided information security training on topics, including password security, phishing awareness, data classification, and incident response, through learning management system software within the Workday platform.

According to University management, training is assigned for all new employees and annually for all existing employees with completion of the training tracked within Workday. Reports are provided to the Human Resources Business Centers (HRBCs)[3] that are responsible for reminding employees to complete the training. University policies[4] require all employees to complete the security awareness

[3] HRBCs provide dedicated human resources services within their respective division and college.

[4] University Policy Number 4-002.5, *Use of Information Technologies and Resources*.

training within 30 days from the date of hire and every 12 months thereafter; however, procedures were not in place to ensure that required security training was completed. According to the policies, employees may lose access to University systems if assigned training is not completed. As of September 16, 2024, 12 percent of University employees had not completed security awareness training and, according to University personnel, the HRBCs had discretion whether to enforce consequences for those who did not complete the training. In response to our inquiry, University management indicated that the Information Security Division would work with the HRBCs to implement procedures for ensuring compliance with University policies.

Effective security awareness training programs require completion by all employees. The lack of security awareness training increases the risk that employees may compromise the confidentiality, availability, and integrity of University data and IT resources.

**Recommendation: To reduce cybersecurity risks, University management should continue efforts to ensure that all employees complete the required security awareness training and enforce appropriate consequences for those who do not timely complete the training.**

### Finding 3: Security Controls – Account Management, 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 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 University data and related IT resources. However, we have notified appropriate University management of the two findings in the areas needing improvement.

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

**Recommendation: We recommend that University management improve IT security controls related to account management and configuration management to ensure the confidentiality, integrity, and availability of University 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 February 2024 through September 2024 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 University IT controls applicable to the Workday Enterprise Cloud Applications (Workday) and University IT infrastructure during the period June 2023 through May 2024, 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 University organizational structure and regulatory requirements; reviewed University procedures, interviewed University personnel, and examined University records to obtain an understanding of University operations related to Workday and IT infrastructure and to evaluate whether University operations were designed properly and operating effectively.
- Evaluated the sufficiency of University controls and observed, documented, and tested key processes, procedures, and controls related to Workday and University IT infrastructure, including

authentication, backup and recovery, configuration of systems, logical controls, logging and monitoring, inventory, security awareness training, and vulnerability management.

- Examined the master subscription agreement between the University and Workday, Inc., effective October 27, 2020; Service Organization Controls 1 Report for the period April 1, 2023, to September 30, 2023; and Service Organization Controls 2 Report for the period October 1, 2022, to September 30, 2023, to determine the sufficiency of the University'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 University logical access controls assigned to the University network and selected network devices, including the periodic evaluation of assigned accounts.
- Evaluated the effectiveness of security management controls for Workday, including University procedures related to the periodic review of assigned user access privileges.
- Evaluated University procedures and examined selected University 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 University procedures and examined selected University 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 University controls over the security administration function for Workday.
- Evaluated selected security settings related to Workday and the supporting University network infrastructure to determine whether authentication controls were configured and enforced in accordance with IT best practices.
- Evaluated University procedures and examined selected scan reports and policies to evaluate the adequacy of University 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 February 28, 2024, within the four default network administrator system groups for the University root domain and one child domain.
- Examined and evaluated the appropriateness of all accounts assigned administrator access privileges, as of April 18, 2024, for five of the six University high risk network devices and as of September 12, 2024, for one of the six University high risk network devices for the University network.
- Examined and evaluated selected University patch management controls for operating systems and network devices to ensure that secure configurations are maintained. Specifically, we examined and evaluated:
    - As of February 28, 2024, the 170 critical servers on the University core business network.
    - As of March 21, 2024, the 6 high risk network devices for the University network.
- Examined and evaluated the appropriateness of all accounts assigned administrative access privileges, as of April 18, 2024, for 15 of the 170 critical servers on the University core business network.
- Evaluated the effectiveness of University 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 the effectiveness of University security awareness training.
- Evaluated University procedures and examined selected records to determine the adequacy of University procedures for maintaining a software asset inventory and ensuring only authorized software is installed on the network.
- Evaluated University procedures and examined selected backup and testing reports to determine the adequacy of the University data recovery procedures to restore University IT assets to a pre-incident trusted state.
- Examined network logging settings and related University reports to determine the adequacy of University 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

UNIVERSITY OF CENTRAL FLORIDA

**Office of the President**
P.O. Box 160002
Orlando, FL 32816-0002

December 4, 2024

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

Dear Auditor General Norman,

Thank you for providing the preliminary and tentative findings from the recent operational audit focused on the University of Central Florida's use of the Workday Enterprise Cloud Applications. We appreciate the thorough review conducted by your office, which highlights areas where we can strengthen our information technology controls, security protocols, and operational effectiveness.

Below, please find our responses to each of the findings outlined in your report. Ensuring the confidentiality, integrity, and availability of our data and IT resources is a top priority for the University of Central Florida. This audit provides valuable insights that will guide us in further refining our processes and controls to align with best practices and safeguard institutional data.

**Finding 1: Application Security Management**

***Recommendation:*** We recommend that University management establish procedures to monitor business process and security group changes so that all changes are appropriately authorized and approved. In addition, management should establish procedures for the periodic review of user Workday 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.

***Management Response:*** The University is developing and implementing a comprehensive framework for monitoring business process and security group changes. This framework will include specific procedures to periodically review Workday access privileges and ensure that all changes to security roles and business processes are authorized and documented.

The University is also establishing procedures for a periodic user access review. These reviews will leverage detailed reports to provide identified approvers with visibility into user access privileges and associated security groups. Access roles and groups will be reviewed on a regular schedule to ensure alignment with business processes and job responsibilities while adhering to the security configuration.

Phone: 407.823.1823 • Fax: 407.823.2264

**Finding 2: Security Awareness Training**

***Recommendation:*** To reduce cybersecurity risks, University management should continue efforts to ensure that all employees complete the required security awareness training and enforce appropriate consequences for those who do not timely complete the training.

***Management Response:*** The University is revising its security awareness training policy to clarify who must complete training and the timeframe to do so. Procedures are also being enhanced to incorporate escalated methods of notification, non-renewal of accounts, and other consequences to enforce timely completion of the training.

**Finding 3: Security Controls – Account Management, Configuration Management**

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

***Management Response:*** We have reviewed our process and available tools to identify current capabilities concerning Configuration Management and are developing an implementation plan with current resources. Account Management controls have been reviewed and new processes for Account Management have been implemented. We anticipate these process enhancements will adequately address this recommendation.

We are grateful for the guidance and partnership your office provides, and we remain committed to addressing these findings swiftly and comprehensively. Should you require additional information or have further questions about our responses or corrective actions, please do not hesitate to contact my office.

Thank you again for your continued support in ensuring excellence in governance and operational effectiveness at Florida's public universities.

Sincerely,

**Alexander N. Cartwright, Ph.D.**
President and Professor of Electrical and Computer Engineering
*University of Central Florida*

Phone: 407.823.1823 • Fax: 407.823.2264