STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2025-081
December 2024

TALLAHASSEE STATE COLLEGE

WORKDAY ENTERPRISE CLOUD APPLICATIONS

Sherrill F. Norman, CPA
Auditor General

Board of Trustees and President

During the period September 2023 through August 2024, Dr. James T. Murdaugh served as President of Tallahassee State College and the following individuals served as Members of the Board of Trustees:

	County
Jonathan A. Kilpatrick, Chair through 8-6-24	Wakulla
Karen B. Moore, Chair from 8-7-24 Vice Chair through 8-6-24	Leon
Eugene Lamb Jr., Vice Chair from 8-7-24	Gadsden
Frank S. Messersmith	Wakulla
Monte Stevens	Leon
Charlie Ward Jr.	Leon
Monesia Brown from 7-26-24[a]	Leon

[a] Trustee position vacant 9-1-23, through 7-25-24.

The team leader was Ellen Henley, CISA, and the audit was supervised by Heidi Burns, CPA, CISA.

Please address inquiries regarding this report to Heid Burns, CPA, Audit Manager, by e-mail at heidiburns@aud.state.fl.us or by telephone at (850) 412-2923.

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

TALLAHASSEE STATE COLLEGE

WORKDAY ENTERPRISE CLOUD APPLICATIONS

SUMMARY

This operational audit of Tallahassee State College (College) focused on evaluating selected College information technology (IT) controls applicable to Workday Enterprise Cloud Applications (Workday) and the College's IT infrastructure and included a follow-up on the findings included in our report No. 2019-002. Our operational audit disclosed the following:

Finding 1: College security awareness training needs improvement to reduce the risk of compromising College data and IT resources.

Finding 2: College IT security controls over account management, data recovery, and vulnerability management could be improved to ensure the confidentiality, integrity, and availability of College data and IT resources.

BACKGROUND

The Tallahassee State College[1] (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 seven 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 uses Workday Enterprise Cloud Applications (Workday) to record, process, and report finance and human resources transactions and student information. The College subscription to Workday using Software as a Service is through Workday, Inc., the software vendor. Workday, Inc. hosts the Workday applications and maintains and manages the supporting information technology infrastructure.

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 preventing and mitigating 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 on how to interact with data and IT resources in a secure manner.

[1] The College was known as Tallahassee Community College until July 1, 2024.

As part of our audit, we examined College procedures, management directives, and related records supporting employee security awareness and skills training during the period September 2023 through August 2024. We found that the College provided, through a vendor-provided solution, training to all employees on various security topics, including phishing, cybersecurity and crime, password security, and ransomware. However, because College personnel had not identified and classified College confidential and sensitive data for data handling procedures, such as secure data storage and transmission, the training did not educate employees about data handling best practices specific to College controls. In response to our inquiry, College management stated that a sensitive data training module would be incorporated in the College security awareness training program in April 2025.

Effective security awareness training programs include instruction about data handling best practices and the causes of unintentional data exposure. The lack of a comprehensive security awareness training program that educates employees about data security 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 implement a comprehensive security awareness training program that informs employees about their responsibilities and the importance of securing College data and IT resources.

Finding 2: Security Controls – Account Management, Data Recovery, 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 account management, data recovery, 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 three findings in the areas needing improvement.

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

PRIOR AUDIT FOLLOW-UP

The College had taken corrective actions for the findings included in our report No. 2019-002.

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 May 2024 through October 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 College IT controls applicable to the Workday Enterprise Cloud Applications (Workday) and College IT infrastructure during the period September 2023 through August 2024, and selected actions subsequent thereto. For those areas addressed by this audit, our audit objectives were to:

- Evaluate 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.
- Determine whether management had taken corrective actions for the finding included in our report No. 2019-002.
- 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 and 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 and 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, logging and monitoring, inventory, security awareness training, and vulnerability management.
- Evaluated the effectiveness of College logical access controls assigned to the College network and selected network devices, including the periodic evaluation of assigned network administrator accounts.
- Evaluated the effectiveness of College monitoring procedures for security provisions implemented by Workday, Inc., including reviewing results of disaster recovery tests conducted.
- Evaluated the effectiveness of logical access controls for Workday, including security administration and College procedures related to the periodic review 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 College Workday, including account creation and changes to security groups and business processes.
- 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 May 15, 2024, within the four default network administrator system groups for the College network domain.
- Examined and evaluated the appropriateness of all accounts assigned administrator access privileges, as of October 14, 2024, for the two high risk network devices for the College network.
- Examined and evaluated selected College patch management controls for operating systems and network devices to ensure that secure configurations are maintained. Specifically, we examined and evaluated:
    - The 18 critical servers on the College network as of June 12, 2024.
    - The 2 high risk network devices for the College network as of May 17, 2024.
- Evaluated the effectiveness of College configuration management controls, including those for establishing and maintaining secure configurations; disabling insecure protocols; implementing firewalls or port filtering to protect network resources; and timely applying software patches and updates and managing device end-of-life.
- Evaluated the effectiveness of College security awareness training.

- 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 College procedures and examined selected backup and testing reports to determine the adequacy of the College data recovery procedures to restore College IT assets to a pre-incident trusted state.
- 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

TSC
TALLAHASSEE
STATE COLLEGE

444 Appleyard Dr.
Tallahassee, FL 32304
(850) 201-6200 | tsc.fl.edu

December 16, 2024

Ms. Sherrill F. Norman, CPA
Auditor General of the State of Florida
Claude Denson Pepper Building, Suite G74
Tallahassee, Florida 32399-1450

Dear Ms. Norman,

Please see the College's response to the list of preliminary and tentative audit findings and recommendations from the Workday Enterprise Cloud Applications dated December 10, 2024.

Finding 1: College security awareness training needs improvement to reduce the risk of compromising College data and IT resources.

Auditor's Recommendation: To reduce cybersecurity risks, College management should implement a comprehensive security awareness training program that informs employees about their responsibilities and the importance of securing College data and IT resources.

College's Response: The College supports this recommendation and have already taken steps to expand our current awareness training to further enhance staff knowledge and the importance of maintaining security controls.

Finding 2: College IT security controls over account management, data recovery, and vulnerability management could be improved to ensure the confidentiality, integrity, and availability of College data and IT resources.

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

College's Response: The College has reviewed its IT security controls related to account management, data recovery, and vulnerability management and we will continually improve our processes to ensure the confidentiality, integrity, and availability of our data and IT resources.

Sincerely,

Jim Murdaugh, Ph.D.
President