TEXAS
The University of Texas at Austin

Workday Information Technology General Controls

May 2024

Office of Internal Audits
UT Austin's Agents of Change

OFFICE OF INTERNAL AUDITS
THE UNIVERSITY OF TEXAS AT AUSTIN

1616 Guadalupe St. Suite 2.302 · Austin, Texas 78701 · (512) 471-7117
audit.utexas.edu • internal.audits@austin.utexas.edu

Executive Summary

Workday Information Technology General Controls

Project Number: 24.011

Audit Objective

The objective of this audit was to evaluate the design and operating effectiveness of information technology (IT) general controls in the Workday environment at The University of Texas at Austin (UT Austin). The primary areas evaluated were:

- Access management
- Change management
- Interface management between Workday and *DEFINE

Conclusion

Overall, UT Austin has effective IT general controls and processes for managing the University's instance of Workday; however, user access reviews are not consistently conducted to help prevent unauthorized access to sensitive employee information.

Audit Observation[1]

Recommendation	Risk Level	Estimated Implementation Date
User Access Reviews	Medium	December 2024

Engagement Team[2]

Mrs. Suzi Nelson, CPA, CIA, CISA, Senior Auditor
Mr. Paul Douglas, CISA, CCSFP, CDPSE, IT Audit Partner, EAG
Mr. Matthew Stewart, CISA, IT Audit Senior Manager, EAG
Mrs. Madelyne Hall, CISA, IT Audit Manager, EAG
Mr. Bentley Greenfield, IT Audit Staff Consultant, EAG

[1] Each observation has been ranked according to The University of Texas System Administration (UT System) Audit Risk Ranking guidelines. Please see page 5 of the report for ranking definitions.
[2] This project was co-sourced with EAG Gulf Coast, LLC (EAG).

Detailed Audit Results

Observation #1 – User Access Reviews

Security administrators do not consistently review access granted to sensitive data within Workday as required by the UT Austin Enterprise Information Technology Solutions team (eBITS) Security Group Biannual Audit procedure[3]. As a result, there is an increased risk of unauthorized access to sensitive employee information stored in Workday.

Although eBITS initiates the user access review process by emailing the responsible staff at the Colleges, Schools, and Units (CSUs), eBITS does not have a process to validate the reviews are completed. Instead, eBITS assumes user access reviews are completed and that access is appropriate unless access changes are requested. Furthermore, reviewers are not required to maintain documentation to demonstrate the reviews were performed and necessary access changes were completed.

Notable Practices

- UT Austin maintains detailed Workday policies and procedures that outline key IT general control requirements.
- eBITS created robust change management documentation and implemented strong IT general controls surrounding the payroll data interface between Workday and *DEFINE.

Recommendation:
UT Austin should strengthen the user access review process by implementing procedures to confirm reviews are performed. This process could include options such as receiving positive confirmation from reviewers or periodically requesting supporting documentation from a sample of reviewers.

Management's Corrective Action Plan:
Based on further analysis using a sample time period, there are 41 people assigned to security roles who have not logged in since January 19, 2024. Managers and merit roles were excluded because managers are not technically assigned; they inherit that role based on reports. Merit roles are only used for annual merit processing each year. Only one individual is assigned to a role with access to confidential or sensitive data defined by the Information Security Office. Thus, it appears that Security Partners in the units are managing role assignments. However, the process needs improvement to mitigate risks for the University.

After reviewing the audit findings and conducting additional analyses, we determined that the Human Resources and eBITS teams will implement the following actions and timing:

1. The sample referenced above will be removed from security roles as of May 31, 2024, and reinstated by request with justification by the units.

[3] Of five supervisory organizations selected for review, none could provide documented completion of user access reviews.

2. Beginning on July 1, 2024, reports will be completed at the end of each calendar quarter to determine who has security access and has not logged onto the system for the prior quarter. These reports will be sent to the units for immediate actions.
3. With new capabilities in Workday going live and implemented in the fourth quarter of 2024, we will build a simple application within Workday that requires Security Partners to certify quarterly that they have reviewed and updated security roles to reflect current access required by individuals to perform in their roles.

In our judgment, this new reporting process and simple application will improve accountability to remain current on security access to Workday.

Responsible Person: Vice President, People and Talent and Executive Director for eBITS

Planned Implementation Date: December 31, 2024

Conclusion

Overall, UT Austin has effective IT general controls and processes for managing the University's instance of Workday; however, user access reviews are not consistently conducted to help prevent unauthorized access to sensitive employee information.

The following table provides a summary of the audit results.

Table: Controls Assessment

Audit Objective	Controls Assessment
Evaluate the design and operating effectiveness of IT general controls for UT Austin's Workday environment.	Generally Effective with Medium Risk Opportunity
Breakdown by area:	
Access Management	Partially Effective with Medium Risk Opportunity
Change Management	Effective
Interface Management	Effective

Background

Workday is a cloud-based enterprise software platform that provides human capital management, financial management, and analytical applications for businesses and organizations. UT Austin is utilizing the Human Capital Management section of Workday that includes a core human resources database, workforce management, recruiting, and benefits.

Scope, Objectives, and Methodology

This audit was conducted in conformance with The Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*. Additionally, we conducted the audit in accordance with Generally Accepted Government Auditing Standards and meet the independence requirements for internal auditors. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions on our audit objectives.

The scope of this review included the current IT general control framework for the Workday environment at UT Austin. Key areas evaluated were:

- Access Management
- Change Management
- Interface Management

Specific audit objectives and the methodology to achieve the objectives are outlined in the table below.

Table: Objectives and Methodology

Audit Objective	Methodology
Evaluate the design and operating effectiveness of IT general controls in the Workday environment.	• Interviewed stakeholders to understand the design of the key IT general controls for access management, change management, and interface management. • Inspected evidence and performed control testing to evaluate the operating effectiveness of key IT general controls for access management, change management, and interface management.

Criteria

The following criteria were used to evaluate Workday IT general controls:

- UT Austin's Information Resources Use and Security Policy (UT IRUSP)
  - Standard 4 – Access Management
  - Standard 5 – Administrative/Special Access Accounts
  - Standard 7 – Change Management
  - Standard 15 – Passwords
- Procedures created by eBITS for Workday logical access and change management (e.g., eBITS Software Change Management and Tenant Guidelines and Security Group Biannual Audit)

The table below summarizes the relevant TAC 202 requirements which were covered during this audit.

Control Family	Control #	Control Name
Access Control	AC-2	Account Management
	AC-3	Access Enforcement
	AC-8	System User Notification
Identification and Authentication	IA-1	Policies and Procedures
	IA-2	Identification and Authentication
	IA-2(1)	Multifactor Authentication to Privileged Accounts
	IA-2(2)	Multifactor Authentication to Non-Privileged Accounts
	IA-4	Identifier Manager
Personnel Security	PS-1	Policies and Procedures
	PS-4	Personnel Termination
	PS-5	Personnel Transfer
Configuration Management	CM-1	Policies and Procedures
	CM-3	Configuration Change Control
	CM-5	Access Restrictions for Change

Observation Risk Ranking

Audit observations are ranked according to the following definitions, consistent with UT System Audit Office guidance.

Risk Level	Definition
Priority	If not addressed immediately, has a high probability to directly impact achievement of a strategic or important operational objective of The University of Texas at Austin (UT Austin) or the UT System as a whole.
High	Considered to have a medium to high probability of adverse effects to UT Austin either as a whole or to a significant college/school/unit level.
Medium	Considered to have a low to medium probability of adverse effects to UT Austin either as a whole or to a college/school/unit level.
Low	Considered to have minimal probability of adverse effects to UT Austin either as a whole or to a college/school/unit level.

In accordance with directives from UT System Board of Regents, Internal Audits will perform follow-up procedures to confirm that audit recommendations have been implemented.

Report Submission

We appreciate the courtesies and cooperation extended throughout the audit.

Respectfully Submitted,

Sandy Jansen, CIA, CCSA, CRMA, Chief Audit Executive

Distribution

Dr. Jay C. Hartzell, President
Mr. Cole Camplese, Vice President of Technology and Chief Information Officer
Ms. Karen Chawner, Director of HR Strategic Workforce Solutions
Mr. Roger Cude, Vice President of People and Talent
Ms. Heather Hanna, Executive Director, Enterprise Business IT Solutions
Mr. Rick Ortiz, Executive Director, Transformation and Strategy Office
Ms. Christy Sobey, Director of President's Office Operations

The University of Texas at Austin Institutional Audit Committee
The University of Texas System Audit Office
Legislative Budget Board
Governor's Office
State Auditor's Office