TEXAS

The University of Texas at Austin

Payment Card Industry (PCI) Compliance

Accounting and Financial Management

March 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

Payment Card Industry Compliance

Accounting and Financial Management
Project Number: 24.012

Audit Objective

The objective of this audit was to determine the effectiveness of controls and processes for conforming with the Payment Card Industry (PCI) Data Security Standard (Security Standard) at The University of Texas at Austin (UT Austin).

Conclusion

UT Austin does not have effective controls and processes to conform with the PCI Security Standard.

Audit Observations[1]

Recommendation	Risk Level	Estimated Implementation Date
University PCI Security Standard Compliance	High	September 2025

Engagement Team[2]

Ms. Autumn Gray, CIA, Assistant Director
Mr. Paul Douglas, CISA, CCSFP, CDPSE, IT Audit Partner
Mr. Matthew Stewart, CISA, Senior Manager
Mrs. Madelyne Hall, CISA, Manager
Mrs. Molly Grant, CIPM, Senior Consultant
Mr. Rudy DeBose, Staff Consultant

[1] Each observation has been ranked according to The University of Texas System Administration (UT System) Audit Risk Ranking guidelines. Please see the last page of the report for ranking definitions.

[2] This project was co-sourced with EAG Gulf Coast, LLC.

Detailed Audit Results

Observation #1 – University PCI Data Security Standard Noncompliance

UT Austin does not have effective processes to conform with the PCI Security Standard[3]. The Cash Management Office (Cash Management) in Accounting and Financial Management has responsibility to provide oversight of PCI Security Standard compliance, but procedures have not been established to confirm College, School and Unit (CSU) merchants[4] are completing the required Self-Assessment Questionnaires[5] (Questionnaire). UT Austin has approximately 230 CSU merchants; however, only 17 submitted a Questionnaire to Cash Management in fiscal year 2023. Some CSU merchants consolidated their Questionnaires, so only nine Questionnaires were submitted. Of the Questionnaires submitted, eight were incomplete or inaccurate.

The following information further illustrates UT Austin's noncompliance with the PCI Security Standard:

- Cash Management maintains a spreadsheet of CSU merchants with details for 231 distinct CSU merchant IDs; however, Cash Management explained the spreadsheet is not an up-to-date list of merchants. An accurate listing of campus merchants is critical to achieving PCI Security Standard compliance.

- During the onboarding of new CSU merchants, Cash Management assigns the unit a Questionnaire type depending on the type of card processing it will be conducting (e.g., e-commerce, face-to-face). The specific card processing activities dictate which attestation is required and which requirements are applicable to the CSU merchant. Cash Management does not periodically reassess assigned Questionnaire types to confirm merchants are still completing the appropriate attestation for their environment.

- Sixty-five of 82 known CSU merchants that were required to have a PCI-approved vendor conduct vulnerability scanning assessments did not meet their submission requirements.

- Third-party service provider[6] relationships are not regularly monitored or reviewed. The third-party relationships, associated network diagrams, and the PCI Security Standard compliance of these providers are not reassessed or reviewed after initial CSU merchant onboarding, as required by the PCI Security Standard.

- The level of resources and support for PCI Security Standard compliance activities varies across CSUs, and CSU merchants are not consistently trained on related requirements. Based on interviews with CSU merchants and process owners, communication with Cash

[3] PCI Security Standard is an information security standard created to protect credit cardholder data and mitigate the risk of payment card fraud. The Security Standard is mandated by major credit card brands.
[4] The PCI Security Standard defines merchant as an entity that accepts payment cards from the major card brands.
[5] Questionnaires are a required self-validation tool used to assess compliance with the PCI Security Standard and to demonstrate established security measures to protect card holder data.
[6] Third-party services providers are vendors that processes online payment card payments on behalf of UT Austin.

Management is minimal after initial onboarding and required annual security training is not provided.

UT Austin has an expansive population of CSU merchants and a complex environment where payment card processing activities are performed. With minimal oversight and coordination in place to confirm CSU merchants are accurately completing and submitting Questionnaires, UT Austin will remain noncompliant with the PCI Security Standard. Furthermore, UT Austin will not meet contractual obligations in the agreement with the UT System payment processing partner, Global Payments Inc., which requires PCI Security Standard compliance. In the instance of a breach of cardholder data on campus, noncompliance with the PCI Security Standard could result in monetary fines, legal action, and damage to the reputation of UT Austin.

Recommendation: Cash Management should develop a structured approach that comprehensively addresses PCI Security Standard compliance requirements. Key areas to consider while developing this approach include:

- Determine responsibility for maintaining PCI Security Standard compliance at UT Austin.
- Identify and implement oversight processes for achieving compliance, such as:
    - Follow-up processes with merchants that have not submitted Questionnaires.
    - Periodic review of CSU merchant inventory for completeness and accuracy.
    - Review of submitted Questionnaire for completeness and accuracy.
    - Review of third-party service provider relationships.
- Develop a roadmap that prioritizes compliance for significant risk areas (e.g., CSU merchants that store cardholder data, network scanning).
- Develop and make available resources such as PCI Security Standard compliance training and ongoing support for CSU merchants and individuals performing PCI compliance activities (e.g., Questionnaires, Cardholder Data Flow Diagram, etc.) to promote better understanding of PCI requirements and responsibilities.

Management's Corrective Action Plan:

Accounting and Financial Management agrees with the identified opportunities and will implement the recommended actions using a phased approach.

Phase 1: Review the CSU merchant inventory list and ensure it is complete and accurate. Prioritize merchants by Questionnaire type and review CSU third-party providers to verify accuracy and compliance. Implementation of phase by September 30, 2024.

Phase 2: Publish electronic CSU merchant onboarding materials. This will include steps to determine Questionnaire type, required third-party provider information, and other materials reviewed by central credit card operations prior to opening a new merchant account. Implementation of phase by February 28, 2025.

Phase 3: Develop and maintain PCI Security Standard compliance training for CSU merchants. A new tool or process will be developed to inform CSU merchants about PCI Security Standard compliance requirements. Training will be mandatory for all CSU merchants.

Cash Management will review CSU merchants annually to verify training is complete, Questionnaires are submitted for all merchants and responses are acceptable, and third-party service providers are accurate and compliant. Implementation of phase by September 30, 2025.

Responsible Person: Director, Treasury, Risk and Payment Information Services

Planned Implementation Date: September 30, 2025

Conclusion

UT Austin does not have effective controls and processes to conform with the PCI Security Standard.

The following table provides a summary of the audit results.

Table: Controls Assessment

Audit Objective	Controls Assessment
Determine the effectiveness of centralized processes to protect cardholder data and achieve PCI Security Standard Compliance	Ineffective with High-Risk Opportunities
Assess the accuracy and dependability of completed Questionnaires.	Ineffective with Medium Risk Opportunities

Additional Considerations for Management

Qualified Security Assessor Tool

Cash Management is engaged in an implementation to replace the Qualified Security Assessor (QSA) tool that assists in the management of PCI Security Standard compliance activities. As Cash Management transitions to the new QSA tool, there is an opportunity to develop more comprehensive compliance reviews and monitoring activities. The new QSA tool should provide capabilities that can offset the need for a manually generated CSU merchant list and has the potential to support CSU merchants in completing Questionnaires.

Industry Standard Changes

The Payment Security Standard is being updated, and PCI Security Standard Version 4.0 will be partially effective in March 2024, and fully in effect as of March 2025. Version 4.0 increases scanning and attestation requirements. These changes may expand necessary PCI Security Standard compliance activities and should be proactively addressed.

Background

Cash Management manages PCI Security Standard compliance for UT Austin. Cash Management provides the needed information and resources for CSUs to become established merchants on campus.

All credit card processing at UT Austin operates under a UT System contractual agreement with the payment processor, Global Payments Inc. (Global Payments). Global Payments facilitates the processing of cardholder data across the UT System. The agreement requires UT Austin to comply with the PCI Security Standard.

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 includes the current PCI Security Standard processes at UT Ausin

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

Table: Objectives and Methodology

Audit Objective	Methodology
Determine the effectiveness of centralized processes to protect cardholder data and achieve PCI Security Standard Compliance	• Interviewed Cash Management personnel to understand how payment card processing and compliance is managed across campus. • Reviewed CSU merchant list to confirm Questionnaire types, CSU merchant levels, payment processors, and third-party service provider information. • Reviewed submitted Questionnaires for accuracy and completeness. • Reviewed Global Payments, Inc. contract.

Assess the accuracy and dependability of completed Questionnaires.	• Tested a sample of CSU merchants for the following: ○ Documented Cardholder Environment Diagrams ○ Annual Questionnaire submission ○ Questionnaire accuracy ○ Understanding of PCI Security Standard requirements ○ PCI awareness and training

Criteria

- Payment Card Industry Data Security Standard
- Global Payments Inc. Contract

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-6	Least Privilege
Awareness and Training	AT-2	Awareness Training
	AT-3	Role-based Training
Program Management	PM-5	System Inventory
Risk Assessment	RA-5	Vulnerability Monitoring and Scanning
System and Communication Protection	SC-7	Boundary Protection
System and Information Integrity	SI-12	Information Management and Retention

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 Sutton Jansen

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

Distribution

Dr. Jay C. Hartzell, President
Ms. Ashley Nemec, Senior Associate Vice President, Financial and Administrative Services
Ms. Lori Peterson, Executive Director and Controller, Financial and Administrative Services
Mr. Daniel Slesnick, Interim Vice President and Chief Financial Officer
Ms. Christy Sobey, Director of President's Office Operations
Dr. Catherine Stacy, Chief of Staff, Office of the Executive VP & Provost
Dr. Sharon Wood, Executive Vice President and Provost
Mr. John Walker, Director III, Office of Accounting
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