The Texas A&M University System Internal Audit Department

Monthly Audit Report
August 11, 2021

TABLE OF CONTENTS

System Internal Audit
THE TEXAS A&M UNIVERSITY SYSTEM

TEXAS A&M UNIVERSITY

ACCOUNTS PAYABLE - TRAVEL

August 11, 2021

Charlie Hrncir, CPA
Chief Auditor

Project #20210202

Overall Conclusion

Internal controls over travel administered by Texas A&M University are operating as intended and in compliance with applicable laws and policies.

Texas A&M University's Financial Management Operations (FMO) administers travel, including the travel card programs, for Texas A&M University, Texas A&M Health Science Center, Texas A&M University at Galveston, Texas A&M University System Offices, Texas A&M System Shared Service Center, and the Texas Division of Emergency Management.

Employee travel expenses for these six A&M System members during the audit period totaled $10,838,746, of which $5,907,607 was paid on travel cards. FMO manages 3,360 travel cards and processed 123,462 employee travel transactions during the audit period.

In August 2020, Texas A&M University implemented Oversight, an automated monitoring software that identifies predefined potential travel card anomalies. Oversight contains supporting documentation to facilitate research of the potential anomalies and tracks the resolutions. The A&M System members use a combination of data from Oversight and Concur, the A&M System's credit card management system, to monitor travel card transactions.

Summary Table

Audit Areas	Controls Assessment
Monitoring Processes	Effective – No Observations
Out-of-Pocket Reimbursement Compliance	Effective – No Observations
Reconciliation Processes	Effective – No Observations
Transaction Approvals	Effective – No Observations
Transaction Card Limits	Effective – No Observations
Transaction Expense Coding	Effective – No Observations
Transaction Expense Reports	Effective – No Observations
Transaction Supporting Documentation	Effective – No Observations
Travel Cardholder Accounts	Effective – No Observations

Basis of Audit

Objective, Scope, & Methodology

The overall objective of this audit was to determine if internal controls over travel administered by Texas A&M University are operating as intended and in compliance with applicable laws and policies.

The audit focused on the following areas:

- Monitoring processes
- Out-of-pocket reimbursement compliance
- Reconciliation processes
- Transaction approvals
- Transaction card limits
- Transaction expense coding
- Transaction expense reports
- Transaction supporting documentation
- Travel cardholder accounts

The audit period was primarily January 1, 2020 to February 28, 2021. Fieldwork was conducted from May 2021 to July 2021. The scope of the audit included travel card and travel expense programs for Texas A&M University, Texas A&M Health Science Center, Texas A&M University at Galveston, Texas A&M University System Offices, Texas A&M System Shared Service Center, and the Texas Division of Emergency Management.

Our audit methodology included interviews, observation of processes, review of documentation, and testing of data using sampling as follows:

Audit Objective	Methodology
Monitoring Processes Determine whether monitoring processes are in place and are being properly performed.	Auditors judgmentally selected a nonstatistical sample of 15 travel card anomalies identified through Oversight and verified the anomalies were properly addressed. Auditors obtained and reviewed a current listing of all unsubmitted and pending travel card expense transactions to verify

Audit Objective	Methodology
	these are being submitted and processed in a timely manner.
Out-of-Pocket Reimbursement Compliance Determine compliance with requirements for out-of-pocket travel reimbursements.	Auditors performed data analysis and judgmentally selected a nonstatistical sample from the 10 reimbursements with the largest number of transactions and dollar amounts per member and employee proportionately across the system members. Documentation was reviewed to determine compliance with out-of-pocket travel requirements: • Allowable purchases • Purchases within limit • Correct coding of expenses • Proper supporting documentation
Reconciliation Processes Determine whether travel card reconciliations were performed in compliance with requirements.	Auditors randomly selected a nonstatistical sample of 30 cardholder transactions using monetary unit sampling to determine if the transactions were properly approved and reconciled to supporting transaction documentation in compliance with reconciliation requirements.
Transaction Approvals Determine whether approvals for travel card expenditures were in compliance with requirements.	Auditors stratified cardholder data into six subpopulations to ensure testing of transactions from vendors, cardholders, and departments with the largest number and dollar amount of transactions. Within each subpopulation, a nonstatistical sample of 30 cardholder transactions was selected using monetary unit sampling. The transactions were tested for compliance with travel card approval requirements.
Transaction Card Limits	Auditors stratified cardholder data into six subpopulations to ensure testing of

Audit Objective	Methodology
Determine whether travel card limits were in compliance with requirements.	transactions from vendors, cardholders, and departments with the largest number and dollar amount of transactions. Within each subpopulation, a nonstatistical sample of 30 cardholder transactions was selected using monetary unit sampling. The transactions were tested for compliance with travel card limit requirements.
Transaction Expense Coding Determine whether coding for travel card expenditures was in compliance with requirements.	Auditors stratified cardholder data into six subpopulations to ensure testing of transactions from vendors, cardholders, and departments with the largest number and dollar amount of transactions. Within each subpopulation, a nonstatistical sample of 30 cardholder transactions was selected using monetary unit sampling. The transactions were tested for compliance with travel card expenditure coding requirements.
Transaction Expense Reports Determine whether expense reports for travel card expenditures were in compliance with requirements.	Auditors stratified cardholder data into six subpopulations to ensure testing of transactions from vendors, cardholders, and departments with the largest number and dollar amount of transactions. Within each subpopulation, a nonstatistical sample of 30 cardholder transactions was selected using monetary unit sampling. The transactions were tested for compliance with travel card expense report requirements.
Transaction Supporting Documentation Determine whether supporting documentation for travel card expenditures was in compliance with requirements.	Auditors stratified cardholder data into six subpopulations to ensure testing of transactions from vendors, cardholders, and departments with the largest number and dollar amount of transactions. Within each subpopulation, a nonstatistical sample of 30 cardholder transactions was selected

Audit Objective	Methodology
	using monetary unit sampling. The transactions were tested for compliance with travel card supporting documentation requirements.
Travel Cardholder Accounts Determine if cardholders are current employees.	Auditors obtained Human Resources' termination report from Business Objects and selected a random sample of 60 terminated cardholders who had travel card transactions during the audit period. Documentation was reviewed to determine if the cardholders were active employees when the card purchases were made.

Controls Assessment Classification

Audit areas highlighted in red in the Summary Table are considered to have significant weaknesses in internal controls. Significant weaknesses include errors, deficiencies, or conditions which result in one or more violations of internal controls, laws, A&M System policies, or member rules. These violations have a high probability for legal consequences, financial consequences, or negative impacts to the organization's reputation. These are situations in which a CEO, provost, vice president, dean, or director need to be involved in the problem resolution.

Audit areas highlighted in yellow in the Summary Table are considered to have notable weaknesses in internal controls. Notable weaknesses include errors, deficiencies or conditions which result in minor to moderate noncompliance with internal controls, laws, A&M System policies, or member rules. These are situations which can and should be corrected at the department or supervisor level.

Audit areas highlighted in green in the Summary Table are considered to have effective internal controls.

Items that were not significant or notable were communicated to management during the course of the audit.

Criteria

Our audit was based upon standards as set forth in the following:

- Texas A&M University System Policies and Regulations
- Texas A&M University Rules and Procedures
- Texas A&M University Travel Card Guidelines
- Texas Government Code 660 Travel Expenses
- Texas Administrative Code Title 34, Chapter 20.413 State Travel Credit Cards
- The Internal Revenue Service Taxable Fringe Benefit Guide – Federal, State, and Local Governments
- Other sound administrative practices

The 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 (GAGAS). 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 based on our audit objectives. The Office of Internal Audit is independent per the GAGAS standards for internal auditors.

Audit Team

Robin Woods, CPA, Director
Danielle Carlson, CPA, CIA, Audit Manager
Debbie Bugenhagen
Holly Giesenschlag, CPA
Nancy Hodgins, CPA

Distribution List

Dr. M. Katherine Banks, President, Texas A&M University
Dr. Mark Weichold, Interim Provost and Executive Vice President, Texas A&M University
Mr. Greg Hartman, Chief Operations Officer, Texas A&M University
Mr. John Crawford, Chief Financial Officer, Texas A&M University
Mr. John McCall, Associate Vice President for Finance and Controller, Texas A&M University
Mr. Clint Merritt, Director, Financial Management Services, Texas A&M University
Mr. Kyle Metcalf, Assistant Director, Financial Management Services, Texas A&M University
Mr. Kevin McGinnis, Chief Risk, Ethics, and Compliance Officer, Texas A&M University
Ms. Margaret Zapalac, Associate Vice President for Risk, Ethics, and Compliance, Texas A&M University
Mr. John Sharp, Chancellor, The Texas A&M University System
Mr. Billy Hamilton, Deputy Chancellor and Chief Financial Officer, The Texas A&M University System
Ms. Janet Gordon, System Ethics & Compliance Officer, The Texas A&M University System
Col. Michael Fossum, Chief Operations Officer, Texas A&M University at Galveston
Ms. Susan Lee, Associate Vice President for Finance and Compliance Officer, Texas A&M University at Galveston
Dr. Jon Mogford, Interim Vice President and Chief Operating Officer, Texas A&M Health
Mr. Jeff Burton, Senior Vice President and Chief Financial Officer, Texas A&M Health
Mr. W. Nim Kidd, Vice Chancellor for Disaster and Emergency Services and Chief of the Texas Division of Emergency Management
Mr. Chuck Phinney, Chief Operating Officer, Texas Division of Emergency Management
Ms. Paula Hanson, Chief Financial Officer, Texas Division of Emergency Management
Mr. Charles Merriweather, Public Information Coordinator and Compliance Officer, Texas Division of Emergency Management

System Internal Audit

THE TEXAS A&M UNIVERSITY SYSTEM

TEXAS A&M UNIVERSITY-CORPUS CHRISTI

INFORMATION TECHNOLOGY

August 11, 2021

Charlie Hrncir, CPA
Chief Auditor

Project #20211501

Overall Conclusion

Internal controls over information technology (IT) at Texas A&M University–Corpus Christi (A&M-Corpus Christi) are operating as intended and in compliance with laws and policies.

The Division of IT is comprised of 78 employees in 28 departments and sub-departments with a combined fiscal year 2021 budget of approximately $12 million. As a centralized IT function, the Division of IT manages over 200 Windows and 300 Linux servers in addition to approximately 5,000 workstations.

Summary Table

Audit Areas	Controls Assessment
Change Management	Effective – No Observations
Compliance	Effective – No Observations
Data Loss Prevention	Effective – No Observations
Disaster Recovery and Backups	Effective – No Observations
Identity and Account Management	Effective – No Observations
Information Security Awareness Training	Effective – No Observations
Logical Security - Linux servers	Effective – No Observations
Logical Security - Windows servers	Effective – No Observations
Logical Security - Windows Workstations	Effective – No Observations
Physical Security	Effective – No Observations
Risk Assessment	Effective – No Observations

Basis of Audit

Objective, Scope, & Methodology

The overall objective of this audit was to determine if controls are in place to ensure the confidentiality, integrity, and availability of information resources.

The audit focused on the following areas:

- Change management
- Compliance
- Data loss prevention
- Disaster recovery and backups
- Identity and account management
- Information security awareness training
- Logical security - Linux servers
- Logical security - Windows servers
- Logical security - Windows workstations
- Physical security
- Risk assessment

The audit period was primarily January 1, 2020 through March 31, 2021. Fieldwork was conducted from May 2021 to July 2021.

Our audit methodology included interviews, observation of processes, review of documentation, and testing of data using sampling as follows:

Audit Objective	**Methodology**
Change Management Verify that changes to IT resources are adequately tracked and approved.	Auditors used professional judgment to select a nonstatistical sample of 20 changes, including high risk and emergency changes. Documentation from the change management system was reviewed for proper categorization of changes, segregation of duties through proper approvals, and final disposition of the changes.

Audit Objective	Methodology
Compliance Determine compliance with the following requirements: • Texas Department of Information Resources (DIR) required Security Controls Catalog items • Texas Administrative Code (TAC) Chapter 202 • Texas Government Code 2054 • Texas A&M University System policies and regulations	Auditors compared published DIR Security Controls Catalog items to the A&M-Corpus Christi required controls. Auditors also reviewed TAC Chapter 202 and Texas Government Code 2054 and tested compliance with applicable requirements. The Division of IT information security program and information security plan were reviewed for compliance with A&M System requirements, including appropriate approvals. Auditors also reviewed the Division of IT information resources risk assessment to determine whether it is complete, comprehensive, and in compliance with A&M System requirements. A listing of IT related purchases over $250,000 since June 5, 2020 was obtained and reviewed for approval by the System Chief Information Officer.
Data Loss Prevention Determine if key assets are being monitored by an approved data loss prevention (DLP) system.	For the sample of servers and workstations selected for logical security testing, auditors verified from system settings whether the university approved DLP application was running on the machines.
Disaster Recovery and Backups Determine whether disaster recovery plans are in place that meet the	Auditors used professional judgement to select a nonstatistical sample of ten servers identified by A&M-Corpus Christi as being

Audit Objective	Methodology
university's contingency planning standards. Determine whether tests of the disaster recovery plans are conducted. Determine if data backups are being performed, tested, and properly protected.	mission-critical from the sample of servers used for logical security testing. Existing disaster recovery plans were reviewed to ensure that the servers were included. In addition, auditors reviewed documentation of recent disaster recovery tests to ensure that they were performed and documented. For the ten servers selected, auditors obtained and reviewed documentation to verify that backups are being performed and tested.
Identity and Account Management Gain an understanding of the processes in place for granting new users access to information resources, modifying existing access when appropriate, and removing access when a business need no longer exists.	Auditors obtained a listing of enabled users from the A&M-Corpus Christi domain and compared it to a listing of recently terminated employees obtained from Workday. For any enabled user accounts not assigned to an active employee, management was asked to review the list and provide the business purpose for these accounts to exist and be enabled. Auditors also reviewed the listing of enabled users for accounts not accessed in over six months.
Information Security Awareness Training Determine if information security awareness training was completed timely.	Auditors obtained a listing of all active A&M-Corpus Christi employees and compared to Train Traq reports to verify that information security awareness training is completed on an annual basis as required.

Audit Objective	Methodology
Logical Security – Linux Servers Verify that logical security controls for Linux servers are operating as intended and in compliance with university procedures and control standards in the following areas: • Password policy • Patch management • Supported operating systems • Less safe practices • Pre-logon banner • Local user accounts • Remote root access	Auditors used professional judgment to select a nonstatistical sample of 19 Linux servers and reviewed system configuration history. Vendor resources were utilized to identify critical security patches released during the audit period.
Logical Security – Windows Servers Verify that logical security controls for Windows servers are operating as intended and in compliance with university procedures and control standards in the following areas: • Password policy • Patch management • Supported operating systems • Supported software versions in use • Anti-virus software • Data loss prevention software • Less safe practices • Pre-logon banner • Appropriateness of domain administrators • MS SQL versions	Auditors used professional judgment to select a nonstatistical sample of 26 Windows servers and reviewed system configuration history. Vendor resources were utilized to identify critical security patches released during the audit period.
Logical Security – Workstations	Auditors used professional judgment to select a nonstatistical sample of 30 Windows workstations and reviewed

Audit Objective	Methodology
Verify that logical security controls for Windows workstations are operating as intended and in compliance with university procedures and control standards in the following areas: • Password policy • Patch management • Supported operating systems • Supported software versions in use • Anti-virus software • Data loss prevention software • Less safe practices • Pre-logon banner • Local administrator accounts	system configuration history. Vendor resources were utilized to identify critical security patches released during the audit period.
Physical Security Determine if physical security and environmental controls are in place and operating as intended in the A&M-Corpus Christi data center.	A remote video walk-through of the A&M-Corpus Christi data center was performed to determine if physical security and environmental controls are appropriate and in compliance with university rules, procedures, and controls.
Risk Assessment Determine if information system risk assessments are being performed in accordance with state, system, and university guidance.	The IT risk assessment summary report was reviewed to ensure that the risk assessments were formally approved by the president. Auditors used professional judgment to select a nonstatistical sample of ten servers to determine if these servers were included in an IT risk assessment.

Controls Assessment Classification

Audit areas highlighted in red in the Summary Table are considered to have significant weaknesses in internal controls. Significant weaknesses include errors, deficiencies, or conditions which result in one or more violations of internal controls, laws, A&M System policies, or member rules. These violations have a high probability for legal consequences, financial consequences, or negative impacts to the organization's reputation. These are situations in which a CEO, provost, vice president, dean, or director need to be involved in the problem resolution.

Audit areas highlighted in yellow in the Summary Table are considered to have notable weaknesses in internal controls. Notable weaknesses include errors, deficiencies or conditions which result in minor to moderate noncompliance with internal controls, laws, A&M System policies, or member rules. These are situations which can and should be corrected at the department or supervisor level.

Audit areas highlighted in green in the Summary Table are considered to have effective internal controls.

Items that were not significant or notable were communicated to management during the course of the audit.

Criteria

Our audit was based upon standards as set forth in the following:

- Texas Government Code
- Texas Administrative Code
- Texas Department of Information Resources Security Control Standards Catalog
- Texas A&M University System Policies and Regulations
- Texas A&M University-Corpus Christi Rules and Procedures
- Texas A&M University-Corpus Christi Security Control Standards Catalog
- Other sound administrative practices

The 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 (GAGAS). 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 based on our audit objectives. The Office of Internal Audit is independent per the GAGAS standards for internal auditors.

Audit Team

Robin Woods, CPA, Director
David Maggard, CPA, Senior Manager
Ana-Lisa Liotta, CIA
Keith Newland, CISA
Bill Williams, CISA

Distribution List

Dr. Kelly M. Miller, President
Dr. Clarenda Phillips, Provost and Vice President for Academic Affairs
Ms. Jaclyn Mahlmann, Executive Vice President for Finance and Administration
Mr. Ed Evans, Senior Associate Vice President for Information Technology and Chief Information Officer
Mr. Kevin Glynn, Chief Information Security and Privacy Officer
Mr. John LaRue, Chief Compliance Officer