UTHealth
The University of Texas
Health Science Center at Houston

16-209 Vendor Master File

We have completed our audit of the vendor master file. This audit was performed at the request of the UTHealth Audit Committee and was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing*.

BACKGROUND

The vendor master file is housed within PeopleSoft Financial Management Solutions (FMS) and includes information on approved vendors, which is used to issue purchase orders and payments for goods and services. As of January 2016, there were approximately 114,000 vendor entries and 14 classifications in the vendor master file. Procurement maintains the vendor master file and monitors/approves changes to vendor information.

OBJECTIVES

The objective of this audit was to determine whether controls over the vendor master file are adequate and functioning as intended.

SCOPE PERIOD

The scope period was November 30, 2014 - December 1, 2015 for all vendor master file activity testing. For the electronic data analysis, the vendor, student, and employee databases were obtained and analyzed as of December 15, 2015.

METHODOLOGY

The following procedures were performed:

- Reviewed a sample of U.S. (25), foreign (25), and student (25) vendors for verification of correctness and appropriate approvals, submittal of supporting W9 and W8 taxpayer forms, and/or debarment checks. A&AS also verified the vendor master file is organized by classification and FMS will not allow the addition/update of vendors with a duplicate Tax ID number.
- Selected a sample of purchase orders over $25,000 and verified the vendor was properly checked for debarment against the Systematic Advocacy Management System (SAMS) prior to payment and deactivated from the vendor master file, if applicable.
- Reviewed a sample of audit trail logs for completeness, and obtained evidence that issues noted in reviews by management were sufficiently resolved.
- Conducted an electronic data analysis to identify anomalies in the vendor master file such as missing information and multiple vendors with the same name, address, phone number, and/or Tax ID. A&AS also compared key fields in the vendor master file with active employee information to detect anomalies. The anomalies were shared with Procurement so further research could be conducted to determine appropriateness. A&AS will conduct verification procedures during the next follow-up period in May 2016.

713.500.3160 phone 713.500.3170 fax
P.O. Box 20036
Houston, Texas 77225
www.uthouston.edu

- Verified formal policies and procedures concerning the vendor master file exist and employee training on vendor code request procedures is conducted on a regular basis.
- Obtained the list of employees with maintenance access to the vendor master file and assessed the appropriateness of access given job titles and responsibilities.

AUDIT RESULTS

A&AS identified an area of improvement related to maintenance access:

- Four employees were determined to have inappropriate maintenance access to the vendor master file.

NUMBER OF PRIORITY & HIGH FINDINGS REPORTED TO UT SYSTEM

None

We would like to thank the staff and management within the Procurement team who assisted us during our review.

Daniel G. Sherman, MBA, CPA, CIA
Assistant Vice President

MAPPING TO FY 2016 RISK ASSESSMENT

Risk (Rating)	R.26 The Vendor Master File is not current or a fraudulent vendor is added (High)

AUDITING & ADVISORY SERVICES ENGAGEMENT TEAM

Assistant Vice President	Daniel G. Sherman, MBA, CPA, CIA
Audit Manager	Brook Syers, CPA, CIA, CFE, CISA
Auditor Assigned	Tammy Tran
End of Fieldwork Date	February 11, 2016
Issue Date	March 10, 2016

Copies to:
Audit Committee
Michael Tramonte
Richard Rawson

Issue #1	A&AS obtained the list of employees with maintenance access to the vendor master file. Of the 10 employees with maintenance access, four (40%) were determined to have inappropriate access.
Recommendation #1	We recommend the inappropriate access maintained by the four employees be removed. Additionally, we recommend Procurement conduct an analysis to determine the root cause of the inappropriate access and actions be taken to address the results of the analysis, if necessary.
Rating	Medium
Management Response	Upon initial review of the security list, of the four individuals identified by the audit to have inappropriate access, only two were determined to be inappropriate. One individual from Student Financial Aid and another from A/R Billing have needed access in the past, when contacted; they both indicated they no longer needed access so were subsequently inactivated. There were two other individuals, one who had previously worked in the Vendor Maintenance area and the other with Student Financial Aid, both had either left UTHealth or transferred to a different department. Upon investigation, it was determined that these two had received a "static" security role instead of a "dynamic" role. When receiving a "dynamic" role, upon termination or transfer, the role is disabled and would need to be applied to reinstate. When receiving a "static" role, the role would be active if the individual returned to UTHealth or transferred. These two individuals have had this role deactivated. Any future assignments of security roles will be done through a "dynamic" role by the security coordinator.
Responsible Party	Richard Rawson
Implementation Date	February 1, 2016