20-201 Cloud Vendor Risk Assessments

We have completed our audit of the cloud vendor risk assessments. 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 Risk Management & Consulting group within Information Technology Security (IT Security) assists in safeguarding UTHealth's data and information technology assets, as well as complying with security regulations, policies, and standards. One of the services offered is a risk assessment/security review of third-party vendors hosting UTHealth data (i.e., cloud vendors). Cloud vendors are assessed against a number of security standards including general, physical, cryptography, network, host, web, and mobile applications. Results of the assessment are communicated to the system owner for review and consideration. If issues identified are deemed high risk, IT Security will follow up and verify remediation.

OBJECTIVES

The objective of this audit was to determine whether controls around cloud vendor risk assessments are adequate and functioning as intended.

SCOPE PERIOD

The scope period was as of March 11, 2020 for the Vendor Risk Questionnaire and as of April 17, 2020 for the Vendor Risk Register/Risk Monitoring Tool spreadsheet.

METHODOLOGY

The following procedures were performed:

- Compared the Vendor Risk Questionnaire to relevant industry guidance, created a crosswalk identifying any anomalies noted, and provided the crosswalk to IT Security for review and consideration.
- Obtained the list of cloud vendor risk assessments conducted, selected a sample, obtained supporting documentation, and assessed for sufficiency in supporting the Vendor Security Risk Assessment Report. Additionally, verified mandatory corrective action plans were completed and sufficient supporting documentation was obtained, if applicable.
- Obtained the Vendor Risk Register/Risk Monitoring Tool spreadsheet and reviewed for timeliness of reassessments.

AUDIT RESULTS

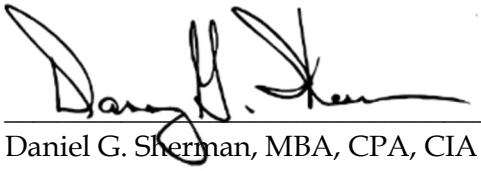
A&AS identified the following areas for improvement:

- Risks reassessments for some cloud vendors were not performed on a timely basis. Additionally, inaccuracies in the Vendor Risk Register/Risk Monitoring Tool spreadsheet were noted.

713.500.3160 phone
P.O. Box 20036
Houston, Texas 77225
www.uth.edu

NUMBER OF PRIORITY FINDINGS REPORTED TO UT SYSTEM
None

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



Daniel G. Sherman, MBA, CPA, CIA
Associate Vice President & Chief Audit Officer

MAPPING TO FY 2020 RISK ASSESSMENT

Risk (Rating)	IT 6 Sensitive UTH data is stored in unsanctioned cloud storage providers. (High) IT 8 Cloud-based application modules fail and result in outages. (High) IT 31 Data stored in the cloud is not backed up and subject to prolonged outage. (High) IT 36 Software solutions have cloud components that add risk and complexity to management of UTH data. Combined with rapid expansion of mobile devices with access to UTH data, the current security program should be broadened to address this. (High) IT 54 Cloud data not backed up at other locations. (Medium) IT 140 Cloud vendors are not adequately assessed for risk. (High)

DATA ANALYTICS UTILIZED

Data Analytic #1	None

AUDITING & ADVISORY SERVICES ENGAGEMENT TEAM

AVP/CAO	Daniel G. Sherman, MBA, CPA, CIA
Audit Manager	Brook Syers, CPA, CIA, CISA, CFE
Auditor Assigned	Kathy Tran, CIA, CFE, CGAP
End of Fieldwork Date	May 12, 2020
Issue Date	May 28, 2020

Copies to:
Audit Committee
Amar Yousif
Beverly Moore

20-201 Cloud Vendor Risk Assessments

<table>
<tr><td>Issue #1</td><td>After the initial cloud vendor risk assessment is performed and services contracted, the risk level assigned by IT Security drives the timeframe of reassessments. Low risk requires reassessment every three years, medium risk is every two years, and high risk is every year.

A&AS obtained the spreadsheet used by IT Security to monitor and manage cloud vendor reassessments. Of the 237 cloud vendors included in the spreadsheet, we noted 108 exceeded their reassessment timeframe:

<table>
<tr><th>Risk Level</th><th># of Vendors</th><th>Days Beyond Timeframe</th></tr>
<tr><td>High</td><td>94</td><td>6 – 966</td></tr>
<tr><td>Medium</td><td>1</td><td>335</td></tr>
<tr><td>Low</td><td>13</td><td>70-252</td></tr>
</table>

Management informed us this was due to staffing issues which are currently been addressed, and reassessments for all high-risk cloud vendors should be completed by August 2020, with medium and low risk vendors to follow.

Additionally, we noted the following inaccuracies in the spreadsheet:
• 53 with an incorrect number of days remaining until the next reassessment.
• 8 with no risk rating indicated.
• 4 with an incorrect risk rating indicated.
• 1 with the assessment date omitted.</td></tr>
<tr><td>Recommendation #1</td><td>We recommend IT Security develop a process to ensure cloud vendor reassessments are performed according to the established timeframe, as well as remediate the backlog of high-risk reassessments. Additionally, we recommend IT Security management periodically review the Vendor Risk Register/Risk Monitoring Tool for accuracy.</td></tr>
<tr><td>Rating</td><td>Medium</td></tr>
<tr><td>Management Response</td><td>IT Security has sufficient staffing to remediate the backlog of high-risk assessments by August 2020.

The Vendor Risk Register/Risk Monitoring Tool has been updated and is now accurate. IT Security management will periodically review it for accuracy and ensure cloud vendor reassessments are performed according to the established timeframe.</td></tr>
<tr><td>Responsible Party</td><td>Beverly Moore, Associate Vice President and Chief Information Security Officer</td></tr>
<tr><td>Implementation Date</td><td>September 30, 2020</td></tr>
</table>