The University of Texas at Tyler

Software Acquisitions Audit

August 2020

THE UNIVERSITY OF TEXAS AT TYLER
OFFICE OF AUDIT AND CONSULTING SERVICES
3900 UNIVERSITY BOULEVARD
TYLER, TEXAS 75799

The University of Texas at Tyler
Software Acquisitions Audit

BACKGROUND

The University of Texas at Tyler (UT Tyler) Office of Audit and Consulting Services completed a Software Acquisitions Audit to determine if departments are following institutional requirements for preapproval when purchasing software. Software that has not been adequately assessed increases the risks related to network security and data protection. Software acquisitions were ranked as a "Critical" risk on the FY 2020 university-wide risk assessment; therefore, this audit was included in the Fiscal Year (FY) 2020 Annual Audit Plan and approved by the Institutional Audit Committee.

AUDIT OBJECTIVE

The objective of the audit was to verify if software acquisitions are following policies for preapproval.

STANDARDS

The audit was conducted in accordance with guidelines set forth in *The Institute of Internal Auditors' Standards for the Professional Practice of Internal Auditing* and *Generally Accepted Government Auditing Standards.*

SCOPE AND METHODOLGY

The scope of this audit included purchases recorded to account codes related to software from September 1, 2018, through February 29, 2020. The procedures conducted included, but were not limited to, the following:

- Reviewing applicable policies and procedures,
- Communicating with management and other employees to gain an understanding of procedures for approving software,
- Obtaining input from the Chief Information Security Officer and Manager of Campus Computing Services (CCS) to identify potential instances of non-compliance and high-risk products,
- Using data analytics to select a judgmental sample, and
- Reviewing approvals and other supporting documentation.

AUDIT RESULTS

The results of our review of 37 purchases identified 20 purchases (54% of the sample) with no documented approval from the Information Technology (IT) department or the Information Security Office (ISO). This included:

- 16 purchases of software, or related renewals or add-ons, and
- 4 purchases of cloud storage service.

We also noted 4 purchases (11% of the sample) that were processed with a "Software" account code that should have used the "Online Subscriptions" account code.

Department personnel have been provided guidance for actions needed related to their specific purchases.

Observations and Opportunities for Improvement:

According to The University of Texas System Audit Office, *A Priority Finding is defined as an issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole. Non-Priority Findings are ranked as High, Medium, or Low, with the level of significance based on an assessment of applicable Qualitative, Operational Control, and Quantitative risk factors and probability of a negative outcome occurring if the risk is not adequately mitigated.*

Legend	
Priority	*A finding is defined as an issue that if not addressed immediately, has a high probability to directly impact achievement of a strategic or important operational objective of UT Tyler.*
High	*A finding that is considered to have a medium to high probability of adverse effects to UT Tyler as a whole or to a significant college or department.*
Medium	*A finding that is considered to have a low to medium probability of adverse effects to UT Tyler as a whole or to a college or department.*
Low	*A finding that is considered to have a minimal probability of adverse effects to UT Tyler as a whole or to a college or department. These findings are communicated separately to management.*

This audit identified 3 High-level findings		
1	High	*Procurement Procedures Manual does not reference required pre-approvals for IT products*
2	High	*Policies for software purchases are not clear and easily accessible*
3	High	*Policies and training for cloud storage services are not clear and easily accessible*

#1: Procurement Procedures Manual - High

The Handbook of Operating Procedures, Series 4.2.1, Best Value Procurement Section D. 3. states: *Detailed procurement procedures are in the Purchasing Procedures Manual on the Financial Services webpage: https://www.uttyler.edu/finserv/purchasing.php.* The Procurement Procedures Manual is the primary resource for purchasing guidelines for employees; however, it does not include references to required approvals for IT purchases, software, or third-party data storage services. Employees who reference the manual exclusively are uninformed of additional approvals required, which can increase information technology and data risks.

Recommendation #1: The Procurement Procedures Manual should include the pre-approval requirements for IT related purchases and links to the applicable policies. It should also include a definition of "Software" which should be processed with account code 63141 and requires pre-approval compared to "On-line Subscriptions" which should be processed with account code 63201 and do not require pre-approval.

Management Response – Manager of Procurement Services / Vice President for Budget and Finance: *We will update the manual with verbiage recommended by the Information Technology and Information Security departments.*

Anticipated Implementation Date: *October 31, 2020*

#2: Policies for Software Approvals - High

The Handbook of Operating Procedures (HOP) is the primary source for University policies and procedures. There is no Handbook of Operating Procedures (HOP) Series specific to Information Technology or Security. The requirements for approval of IT related purchases are described on the, Information Technology website which states:

- *All IT related purchases need to be reviewed by IT before the purchase is made or the PO is created. This is necessary to assure our IT department can provide necessary support for the item and that the item will not compromise university data or resources. This includes any item that would need IT Support for installation or support such as software, apps, computers, laptops, tablets, monitors and any peripheral equipment such as keyboards, mice, web cams, headphones, printers, etc.*

The Information Security Office website includes an Information Security Policy which states:

- *Any software that is not directly related to conducting University business should be reviewed and approved by CCS before being installed by the user.*

The IT department approves requests for standard software products and forwards other requests to the ISO for a detailed review. The ISO sends a Risk Assessment Survey to departments to provide information to enable the ISO to assess the risks related to the specific product requested. As noted above, documented approval was not on file for 16 software purchases. This was primarily caused by lack of awareness of the policies and confusion in the policy verbiage. This increases the risk that employees are not obtaining required approvals, thereby increasing information technology and data risks.

Recommendation #2a: A HOP Series should be developed for Information Technology and Security with links to applicable webpages and policies. The Information Security Policy verbiage should be clarified that all purchases should be for University business and include information related to approvals, including renewals and add-ons of previously approved products.

Management Response – Chief Information Security Officer: *I will submit verbiage to be included in the HOP that include links referencing existing Information Security policies on UT Tyler's website. Policy verbiage will be clarified as suggested.*

Anticipated Implementation Date: *January 31, 2021*

Recommendation #2b: The Information Technology department should clarify the verbiage on their website regarding required approvals. They should also collaborate with the ISO to consider developing a pre-approved list of software that can be posted on the website.

Management Response – Manager of Campus Computing Services / Vice President for Technology: *Policy verbiage will be clarified as suggested. Technology Support will work with the ISO to develop a pre-approved list of software that is posted on the website.*

Anticipated Implementation Date: *January 31, 2021*

#3: Policies for Cloud Storage - High

UT Tyler websites contain policies and training modules related to cloud storage as follows:

- Information Security Policy, Section 15.1, states: *All vendors that host or access University Data must be pre-approved by the Information Security Office prior to use and are subject to a risk assessment performed by the ISO. This includes acquisition (paid or free) and use of external services such as cloud storage, application or communication providers.*
- The Information Resources Acceptable Use and Security Policy Agreement states: *"Users who store University Data using commercial cloud services must use services provided or sanctioned by University, rather than personally obtained cloud services.*
- Information Technology website states: *All vendors that host or access University Data must be pre-approved by the Information Security Office prior to use. This includes acquisition (paid or free) and use of external services such as cloud storage, application or communication providers.*
- Employee Compliance Training includes a Module related to Information Security which states:
  - *Only University sanctioned cloud storage and application may be used to store confidential University data. Sanctioned solutions include OneDrive for Business and Office 365-O365.*
  - *Storing Category I & Category II on non-sanctioned third-party services is prohibited. Examples provided include Google Drove, Google Docs, and Dropbox.*
  - *Users are permitted to store Category III data on non-sanctioned cloud storage and applications. Examples of Category III data provided include Departmental websites, Course catalog and curriculum information, and Publicized research findings.*

As noted above, documented approval was not on file for 4 purchases of cloud storage. The various policies and the training materials are not in agreement, causing confusion related to required approvals. This increases the risk that employees are not obtaining required approvals and are storing data on unapproved services, thereby increasing information technology and data risks.

Recommendation #3: The policies and training verbiage should be clarified and communicated to the campus community.

Management Response – Chief Information Security Officer: *We had considered changing the policy to allow storing Category III data on non-sanctioned cloud services, and the training material reflected that change. The policy was never changed however, and after discussing with Audit and IT, we have decided the best course of action would be to not change the policy. We will update the training material to reflect the current policy.*

Anticipated Implementation Date: *November 30, 2020*

CONCLUSION

Clarifying and communicating policies and training related to software acquisition and cloud storage services should strengthen internal controls related to information technology and security, and therefore reduce the related risks.

We sincerely appreciate the assistance of the Information Security Office, the Information Technology Department and Financial Services during this project.