THE UNIVERSITY OF TEXAS
PERMIAN BASIN

Report on Roles & Permissions - Third Party Applications

January 2022

Office of Internal Audit
4901 E. University Boulevard
Odessa, Texas 79762

Executive Summary

We have completed our audit over Roles and Permissions – Third Party Applications for UT Permian Basin, (UTPB) as included in the approved Audit Plan for fiscal year 2020.

The objective of our audit was to evaluate user access, assigned roles and permissions, and segregation of duties within external third-party applications.

Conclusion

Testing revealed instances of users assigned inappropriate roles within the Touchnet application; and that two users in the EAB application retained access and permissions after end of employment.

Audit Finding	Risk Level	Detail
1. **Users in the Touchnet application were assigned inappropriate roles resulting in unnecessary permissions and an inadequate segregation of duties.**	High Risk	Page 3
2. **Two users in the EAB application retained their access and related permissions after end of employment.**	Medium Risk	Page 5

Finding 1 – Users in the Touchnet application were assigned inappropriate roles resulting in unnecessary permissions and an inadequate segregation of duties.

High Risk

Touchnet is UTPB's financial commerce software. In our review over roles and permissions in Touchnet we noted several users were inappropriately assigned administrator roles which were not necessary for performance of job duties. Administrative access grants users' permissions in most or all areas within an application; consequently, there is no segregation of duties between users with administrator roles.

Proper assignment of user roles and permissions is an important control. Failure to restrict access to appropriate levels can result in more users with access to confidential financial information; this increases the potential risks related to misuse of financial information or misappropriation of financial assets. Inadequate segregation of duties makes it difficult to prevent and detect fraud.

We discussed our findings and the need to limit administrator roles with the Director of Accounting; following that discussion administrator access was removed from users where it was not required to perform job duties. The changes made to limit administrative access addressed the segregation of duties issue within the Touchnet application.

Recommendation

A detailed review should be performed over the permissions currently assigned to each user; adjustments should be made as needed so that only necessary permissions are retained. As a preventative control, assignment of roles and permissions should be limited to the Director and one other designated manager. A predetermined list of the permissions required for each position could be used as an aid when adding new users.

Finding 1 – Users in the Touchnet application were assigned inappropriate roles resulting in unnecessary permissions and an inadequate segregation of duties.

High Risk

Management's Response/Action Plan

As of 11/23/2021, the Director of Accounting and the Bursar are the only people that have the User Administrator role within TouchNet. This role assigns roles to new users. No new users will be given this role. Also, there are two ITS staff members that have administrator access for Marketplace uStores. This role assigns roles to new uStore users. To ensure that the correct roles are given to new users on TouchNet, the Bursar will review roles with the Director of Accounting before permissions are granted.

Target Implementation Date

The changes were implemented 11/23/2021.

Responsible Party

The Director of Accounting

Finding 2 – Two users in the EAB application retained their access and related permissions after end of employment.

Medium Risk

The Education Advisory Boards Student Success Collaborative application (EAB) is UTPB's student relationship management software. The EAB application houses confidential student information such as advising notes, progress reports, and grade point averages. In our review over user roles and permissions within the EAB application we noted that two users no longer employed with the University have retained their access.

Termination of system access immediately upon the end of employment is an important preventative control. Student education records are private, and the information is protected by the Family Educational Rights and Privacy Act (FERPA). There is always a risk that users could inadvertently, or with malicious intent, leak or misuse information; unauthorized users maintaining access increases this risk. Misuse of confidential student information would be a violation of FERPA.

Recommendation

A review over the process for removal of terminated employee access should be performed to identify why it is not functioning as it should. Changes to correct the issue should be made or a new process should be developed and employed.

Finding 2 – Two users in the EAB application retained their access and related permissions after end of employment.

Medium Risk

Management's Response/Action Plan

We have removed the problem access pointed out for the two users, and we are reviewing student permissions. We are preparing a plan for a yearly clean-up of roles and access to take place each July.

Target Implementation Date

July 2022

Responsible Party

Dean's Office

Background, Audit Objective, and Scope & Methodology

Background

In the annual risk assessment for fiscal year 2020 the possibility that users within a third-party application (TPA) may be assigned inappropriate roles resulting in unnecessary/excessive permissions, leading to an inadequate segregation of duties, was determined to have an overall risk score of "high". An audit of Roles and Permissions - Third Party Applications was approved by UTPB's Audit Committee as part of the FY 2020 Audit Plan.

Audit Objective

The objective of our audit was to evaluate employee access, assigned user roles and permissions, and segregation of duties with external third-party applications.

Scope & Methodology

Using a risk-based approach we selected four TPA's for testing;

1) **Raisers Edge:** UTPB's cloud-based fundraising and donor management software that: houses donor information (physical addresses, e-mail addresses, phone numbers); maintains records over donations/gifts; and processes online credit card payment related to donations/gifts, etc.
2) **Touchnet:** UTPB's commerce software that: includes a cashiering application which integrates and centralizes in-person payments, POS payments, and departmental deposits; allows for transfer of campus payment transactions to financial institutions; allows for departments to set up online stores and accept credit cards for services or goods offered within their department; and provides the functionality that allows students to view account balances, make payments, set up payment plans, etc.

Background, Audit Objective, and Scope & Methodology, cont.

Scope & Methodology, cont.

3) **Visualzen, VZ Orientation (VZO):** UTPB's online orientation management software.
4) **EAB's Student Success Collaborative (EAB):** UTPB's student relationship management software.

We reviewed employee roles and permissions for the selected TPA's and performed the following procedures:

- Reviewed policies associated with security controls according to TAC 202.76 of the Texas Administrative Code; UTS 165, "Information Resources Use and Security Policy"; and UTPBs Information Security Policies
- Gained an understanding of the procedure for assigning roles and permissions for each TPA tested
- Reviewed list of user(s) access to confidential or sensitive data and evaluated whether user access is appropriate
- Determined whether segregation of duties is adequate based on the level of access for various user types within the TPA

We conducted this performance audit in accordance with *Generally Accepted Government Auditing Standards*. 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. We also conducted this audit in accordance with the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*; and with guidelines set forth in UTS 129.

The UTPB Office of Internal Audit meets the independence requirements set forth in *Generally Accepted Government Auditing Standards (GAGAS).*

Other Discussion Item

From our test work we noted instances where user access within a TPA was maintained after end of employment (see finding 2). While there are risks that an employee's departure isn't communicated to Information Technology Services (ITS), or Human Resources in a timely manner, this has been previously addressed - primarily in relation to PeopleSoft access – in revised procedures being implemented.

With regard to applications/programs from third party providers (i.e., applications not directly supported by ITS) we met with management to discuss possible solutions to mitigate the risks associated with users maintaining access and permissions when an employee's job duties have changed, or there has been a change in employment status. We discussed the need to notify the appropriate level of management in the affected user's department, as well as ITS, that a change to or termination of access within that TPA may be required.

Risk Ranking Criteria for Audit Findings

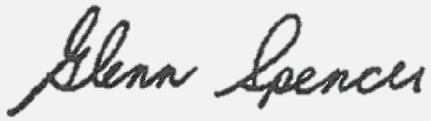
Risk Definition	Risk Level
An issue or condition, if not addressed immediately, has a high probability to directly impact achievement of a strategic or important operational objective of UT Permian Basin or UT System as a whole	Priority Risk
Risk that is considered to be substantially undesirable and results in a medium to high probability of significant adverse effects to UT Permian Basin either as a whole or at the college/department/unit level	High Risk
Risk that is considered undesirable and has a low to medium probability of adverse effects to UT Permian Basin either as a whole or at the college/department/unit level. Without appropriate controls, the risk will occur some of the time	Medium Risk
Considered to have minimal probability of adverse effects to the UT institution either as a whole or at the college/ school/unit level. Even with no controls, the exposure to UT Permian Basin will be minimal	Low Risk

Distribution

To: Dr. Sandra Woodley, President

cc: Felecia Burns, Director of Accounting
Wendell Snodgrass, Vice President of Advancement
Michael Frawley, Dean of Student Success
Adrian Lodge, Director of Student Life
Audit Committee Members

From: Glenn S. Spencer, CPA, CGMA
Chief Audit Executive



Auditor in Charge

Erin Hamilton, Auditor III

External Distribution

UT System Audit Office
State Auditor's Office
Office of the Governor – Budget and Policy Division
Legislative Budget Board