TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER EL PASO
Office of Institutional Compliance

Texas Tech University Health Sciences Center El Paso
Institutional Compliance Procedure

Enterprise Risk Assessment Procedure	**Policy:** COMP 18 PRO
	Effective Date: January 1, 2017
References: 164.308(a)(1)(ii)(A)	
TTUHSC El Paso Institutional Compliance Website: http://elpaso.ttuhsc.edu/compliance/	

Procedure Statement

To guide the compliance staff in their duties of performing a systematic review of significant university functions. This procedure establishes a standardized mechanism for the Compliance Department to actively participate in the required enterprise risk management activities described by the Texas Tech University System Board of Regents (BOR).

Scope

This policy applies to activities associated with Texas Tech University Health Sciences Center El Paso's (TTUHSC El Paso's) Compliance Department.

Procedure

Risk Area Selection

With the exception of the annual Health Insurance Portability and Accountability Act (HIPAA) security risk assessment, risks can be identified by a variety of means, which include the compliance annual risk assessment, areas of concern brought forward by senior leadership, areas that are receiving heightened government oversight or areas submitted by various committees throughout the organization.

Risk Assessment Tools

If there is not an existing tool, such as the HIPAA security risk assessment tool, the compliance staff members will create a tool using the following methodology.

1. Staff members will thoroughly research the requirements associated with the risk area. The research will include a review of federal regulations, state regulations, BOR Regents' Rules, existing university policy.

2. The rules will be compiled into a table that will allow staff members to determine if the existing procedures coincide with the requirements of the statutes, rules and policies. The formatting of the tool will be similar to that used during the compliance-related audit process.

Risk Assessment

1. Once the Compliance Department staff has determined the area(s) of focus for the risk assessment, they will work with process owners to arrange a mutually agreeable time to perform an opening conference and begin risk assessment fieldwork.

a. Compliance staff members will first conduct an entrance conference to discuss the proposed risk assessment in detail, including scope, predicted methodology and how the risk assessment results will be presented. The entrance conference allows the operational owners to address any questions or concerns they might have and to identify any additional items they feel should be added to the risk assessment.

2. Once the entrance conference has been completed, the compliance staff members will proceed with the risk assessment. It must be noted that members from the functional department will be called upon to provide information, access to systems, or whenever assistance is necessary, to complete the risk assessment.

3. Compliant areas – Staff will collect documentation of compliance with each element listed on the risk tool and scan or save an electronic copy in the appropriate folder in the "batman drive."

4. Non-compliant areas – Staff will document in detail why the area does not meet the standards, and add comments and or recommendations to the risk tool to aid in final scoring and the final report.

Documentation of the Risk Assessment

1. All risk assessments will be categorized in accordance with TTUHSC El Paso's enterprise risk management methodology. The major categories of risk are:

   a. ***Strategic*** – risks threatening organizational reputation, constituent relationships, ability to generate funds, goal achievement, etc.

   b. ***Operational and Information Technology*** – risks threatening continuity of activities, safety and security, information technology operations, physical infrastructure, process efficiency, program effectiveness, etc.

   c. ***Financial*** – risks threatening resources, financial structure, ability to meet future financial needs, financial reporting, etc.

   d. ***Compliance*** – risks of non-compliance with legal, regulatory, contractual, accreditation body, NCAA, or other requirements

2. The risk area(s) will be categorized into TTUHSC El Paso's rating scale, which includes four domains: impact, likelihood, preparedness and velocity.

   a. ***Impact*** refers to the potential consequences to the organization, should a loss occur. Impacts may range from negligible to significant across the four risk categories, and one event could generate multiple impacts. While no scale can encompass every potential impact, we have included such potential consequences as reputational damage; financial impacts; interruption to activities; loss of

information technology or physical infrastructure; compliance violations; constituent dissatisfaction; persistent negative media coverage; safety and security concerns; and loss of workforce, students, or patients, and the like.

b. ***Likelihood*** of a risk occurrence may range from extremely unlikely to very likely, and should be assessed in light of the effectiveness of existing controls, as they are known.

c. ***Preparedness*** refers to the organization's readiness to deal with a risk. Preparedness should be assessed based on the existence and effectiveness of such aspects as prevention or detection controls, recovery arrangements, backups, response plans, communication plans, insurance, and notifications to constituents, emergency management planning and the like.

d. ***Velocity*** refers to how quickly a risk could impact the organization. For example, an information technology cyberattack could have an instantaneous impact, while a legislative change may only impact the organization months or even years later.

Reporting

1. Once the risk assessment tool has been completed, the staff members will create a draft report of the findings. Depending on the size and scope of the risk assessment, the findings may be categorized into one or more and distinct chapters. The findings will be discussed with the department/operational owners of the findings during an audit exit conference. The exit conference will give operational owners the ability to accept or refute the stated findings and to assist in of identifying the individuals that will be responsible for the development of the corrective action plan.

2. The final report will be presented to the departmental/operational owners, and the appropriate committees, which will include the institutional compliance committee, the enterprise risk management committee, senior management and other individuals identified has process owners.

Frequency of Review

This procedure will be reviewed June 1 of every even-numbered year by the institutional compliance officer, with recommendations for revisions forwarded to the Institutional Compliance Committee.

Review Date:

Revision Date: January 1, 2017