TEXAS TECH UNIVERSITY SYSTEM™

MEMORANDUM

TO: Chancellor Robert L. Duncan
Dr. Rick Lange, TTUHSC EP President
Dr. Brian May, ASU President
Dr. Tedd Mitchell, TTUHSC President
Dr. Lawrence Schovanec, TTU President

FROM: Enterprise Risk Management Committee
Steve Bryant, TTUS Managing Director of Risk Management
Dale Dunn, MD, TTUHSC Executive Associate Dean, School of Medicine
John Huffaker, TTUS Vice Chancellor and General Counsel
Michael Molina, TTUS Vice Chancellor of Facilities Planning & Construction
Noel Sloan, TTU Chief Financial Officer & VP for Administration & Finance
Frank Stout, TTUHSC EP Vice President of Operations
Kim Turner, TTUS Chief Audit Executive
Angie Wright, ASU Vice President for Finance & Administration

DATE: September 9, 2016

SUBJECT: Enterprise Risk Management

Committee Charge and Summary

In Spring 2016, Chancellor Duncan presented his strategic initiatives to the Board of Regents, one of which was the implementation of Enterprise Risk Management processes across the Texas Tech University System. To assist with implementation, Chancellor Duncan appointed a committee with the following charge: "To oversee the development of Enterprise Risk Management (ERM) processes across the Texas Tech University System and to facilitate timely reporting of ERM information to executive management and the Board of Regents."

In fulfillment of this charge, we have developed a framework and adopted consistent concepts to be used throughout the Texas Tech University System in the further development and implementation of ERM processes. The following sections include our recommendations for definitions, rating scales, and other concepts to be utilized throughout the Texas Tech University System. We have also included some recommendations related to approach and reporting as the institutions begin to develop their implementation strategy.

Definitions and Rating Scales

Definition of Enterprise Risk Management

Enterprise Risk Management (ERM) assesses and defines actions to be taken by the Board of Regents, Texas Tech University System Administration and/or the component institutions to identify, mitigate, and monitor risks that threaten the achievement of strategic plan goals and/or continuing operational activities.

Statement of Risk Attitude

Texas Tech University System will continuously seek out innovation in the way we deliver our mission while ensuring that all decisions are informed by an understanding of the uncertainties we face as an organization. We will continuously seek out those opportunities that can best strengthen our core values. While it is not possible or even desirable to eliminate all risk, we will not tolerate any risks that:

- Willfully expose students, employees, or other people to unsafe environments or activities;
- Intentionally violate laws, regulations, contractual obligations, or other externally imposed requirements; or
- Result in unethical behavior.

Major Categories of Risk

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

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

Financial – Risks threatening resources, financial structure, ability to meet future financial needs, financial reporting, etc.

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

Rating Scales

We have developed rating scales to rank each identified risk on four domains: impact, likelihood, preparedness, and velocity. The rating scales are included as Attachment 1, with summaries listed below.

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 contemplate 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; loss of workforce, students, or patients, and the like.

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.

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.

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, notifications to constituents, emergency management planning, and the like.

Considerations for Implementation

The initial ERM report from each component (i.e., each institution and TTUSA) will be provided to the Board of Regents in February 2017 in conjunction with the annual strategic planning meeting. To assist with this short timeline, we have developed some quick-start strategies to assist in the initial generation of information.

We recommend that each component plan to initially report on the two most threatening risks in each category. Determining the two most significant risks in each category will likely involve applying the rating scales to more than two risks and determining which two are most important to include. Later, as ERM processes mature and include information from throughout the institutions, the list of the most significant risks will also mature and may include more or less than two in each category. While it is not intended to be all-inclusive, Attachment 2 herein is a list of potential major risks to spur discussion and brainstorming during the risk assessment process.

Reporting to the Board of Regents

We believe a concise approach to reporting to the Board will be most desirable and have developed a template for all components to use in ERM reporting. This format will provide condensed information about the most significant risks in a dashboard format, which will facilitate comparisons and easier digestion of information.

Attachment 3 includes a sample heat map in the format we recommend. We have also developed an Excel tool where ratings for each risk can be entered and the heat map automatically produced. We have provided this tool to the institutional representatives on this committee.

Attachment 1: Rating Scales

IMPACT					
		Financial	Operational	Compliance	Strategic
Level		Resources, financial structure, ability to meet future financial needs, financial reporting	Continuity of activities, safety and security, IT operations, physical infrastructure, process efficiency, program effectiveness	Legal, regulatory, contractual, accreditation body, NCAA, or other requirements	Organizational reputation, constituent relationships, ability to generate funds, goal achievement
1	Minor	Insignificant financial impact	Negligible interruption to activities. Minor information technology event. No loss of infrastructure. Negligible effect on efficiency and effectiveness.	Minor incidental compliance violations	No discernable negative impact to reputation and/or goal achievement. Minor media coverage. Negative effect on constituent satisfaction or relationships.
2	Moderate	Notable financial impact	Brief or limited interruption of activities. Notable information technology event. Minor loss of infrastructure. Moderate loss of process efficiency and/or program effectiveness.	Repetitive or systemic compliance violations	Notable temporary negative impact to reputation and/or goal achievement. Some media coverage. Constituent dissatisfaction or strain on relationships.
3	Major	Material financial impact	Major interruption of activities. Major information technology event. Localized loss of infrastructure. Moderate safety or security concerns.	Major compliance violations	Major negative impact to reputation and/or goal achievement. National media coverage. Constituent dissatisfaction and loss of relationships.
4	Severe	Financial impact threatens solvency or ability to continue operations	Extensive interruption of activities. Significant information technology event. Significant loss of infrastructure. Significant safety or security concerns.	Significant, chronic, and/or pervasive compliance violations	Significant negative impact to reputation and/or goal achievement. Persistent national and/or international media coverage. Significant loss of workforce, patients, students and/or donor base.

Attachment 1: Rating Scales (continued)

LIKELIHOOD		
Given the potential risks and effectiveness of existing controls, how likely is it that we will experience a risk event under the activity?		
Level	**Category**	**Average Frequency**
1	Very unlikely	Remote possibility of occurrence. (e.g., More than 3 years out)
2	Unlikely	More than remote possibility of occurrence (e.g., Every 1 to 3 years)
3	Likely	Happens with some frequency (e.g., Likely to happen this year)
4	Very likely	Expected to happen or happens often (e.g., Several times per year)

VELOCITY	
How quickly can the risk impact the organization?	
Level	**Category**
1	One Year or Greater
2	Weeks to Months
3	Days to Weeks
4	Hours to Days

PREPAREDNESS		
Prevention, detection, recovery, backups, response plans, communication plans, insurance, notifications, emergency management planning		
Level	**Category**	**Description**
1	Very Prepared	Significant preparation efforts and risk mitigation strategies are in place. Very few identified issues and/or opportunities for improvement/enhancement exist.
2	Prepared	Moderate preparation efforts and risk mitigation strategies are in place. Some identified issues and/or opportunities for improvement/enhancement exist. Minimal possibility of other unidentified issues or opportunities.
3	Somewhat Prepared	Minimal preparation efforts in place. Major issues and/or opportunities for improvement/enhancement exist. Moderate possibility of other unidentified issues or opportunities.
4	Very Unprepared	Virtually no preparation is in place. Significant identified issues and/or opportunities for improvement/enhancement exist. Strong possibility of other unidentified issues or opportunities.

Attachment 2: Potential Major Risks

This list is intended to spur brainstorming about major institutional risks. It is not intended to be all-inclusive, nor to take the place of an institutional risk assessment.

Strategic

- Negative reputational event (usually stems from not managing other major risks)
- Governance breakdowns – arguably the most significant reputational risks stem from governance issues (e.g., Penn State)
- Scaled back public funding (e.g., state appropriations, federal research funds, Medicaid reimbursements) pushes more of the burden to students and intensifies pressure to cut costs
- Loss or lack of institutional accreditation
- Declining enrollments
- Strained town/gown relations
- Online offerings (including free courses) may impact the traditional university setting

Operational and Information Technology

- Cybersecurity threats
- Privacy mishaps or information losses (e.g., patient/student information, credit cards, SSNs, etc.)
- Recruitment and retention of faculty and staff
- Catastrophic event (e.g., natural disaster, active shooter, etc.)
- Facility optimization risks and opportunities (e.g., aging facilities, increasing deferred maintenance cost, opportunity for private partnership/revenue generation, etc.)

Financial and Reporting

- Investment underperformance
- Failed fundraising campaign
- Ineffective use of resources (e.g., funding declining programs vs. strategic/growth initiatives)
- Inefficient use of resources (e.g., duplication of the same service across multiple areas)
- Data analytics are not used strategically
- Data is misreported to authorities
- State budget cuts
- Fraud

Legal and Regulatory Compliance

- Loss of accreditation of an institution, college, school, or program
- Research compliance violations (e.g., conflicts of interest, research misconduct, etc.)
- Health and safety violations threaten physical safety and security (e.g., lab safety, construction safety issues, etc.)
- Healthcare compliance violations (e.g., HIPAA, Medicare/Medicaid payment rules, etc.)
- Major NCAA violation
- Title IX issues

Attachment 3: Sample Heat Map

Each component will prepare a heat map similar to this one depicting each of its eight highest risks on the four rating scales of impact, likelihood, velocity, and preparedness.