TEXAS TECH UNIVERSITY SYSTEM™

Enterprise Risk Management

Gary Barnes
Vice Chancellor & Chief Financial Officer

February 23, 2017

ERM Update/Development

- Introduced in Spring 2016
- ERM Strategic Initiative Committee
- TTUSA to oversee development of ERM
- Facilitate timely reporting and uniform implementation

Initial ERM Committee

Kim Turner
Chief Audit Executive, TTUSA

Steve Bryant
Managing Director Office of Risk Management, TTUSA

Dale Dunn, MD
Executive Associate Dean, School of Medicine, TTUHSC

John Huffaker
Vice Chancellor General Counsel, TTUSA

Michael Molina
Vice Chancellor Facilities Planning & Construction, TTUSA

Noel Sloan
CFO & VP Financial Affairs, TTU

Frank Stout
VP Operations & COO
TTUHSC El Paso

Angie Wright
VP Finance & Administration, ASU

Committee Accomplishments

- Definition of ERM
- Statement of Risk Attitude
- Major Categories of Risk
- Rating Scales
- Reporting Guidelines

Definition of ERM

Enterprise Risk Management (ERM) is a comprehensive program to identify and proactively manage real and potential threats as well as opportunities that may affect TTUS component institutions. ERM is a powerful tool in strategic planning, resource allocation, risk management and audit planning.

Statement of Risk Attitude

TTUS 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.

While it is not possible or even desirable to eliminate all risk, we will not tolerate 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, 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

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.

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.

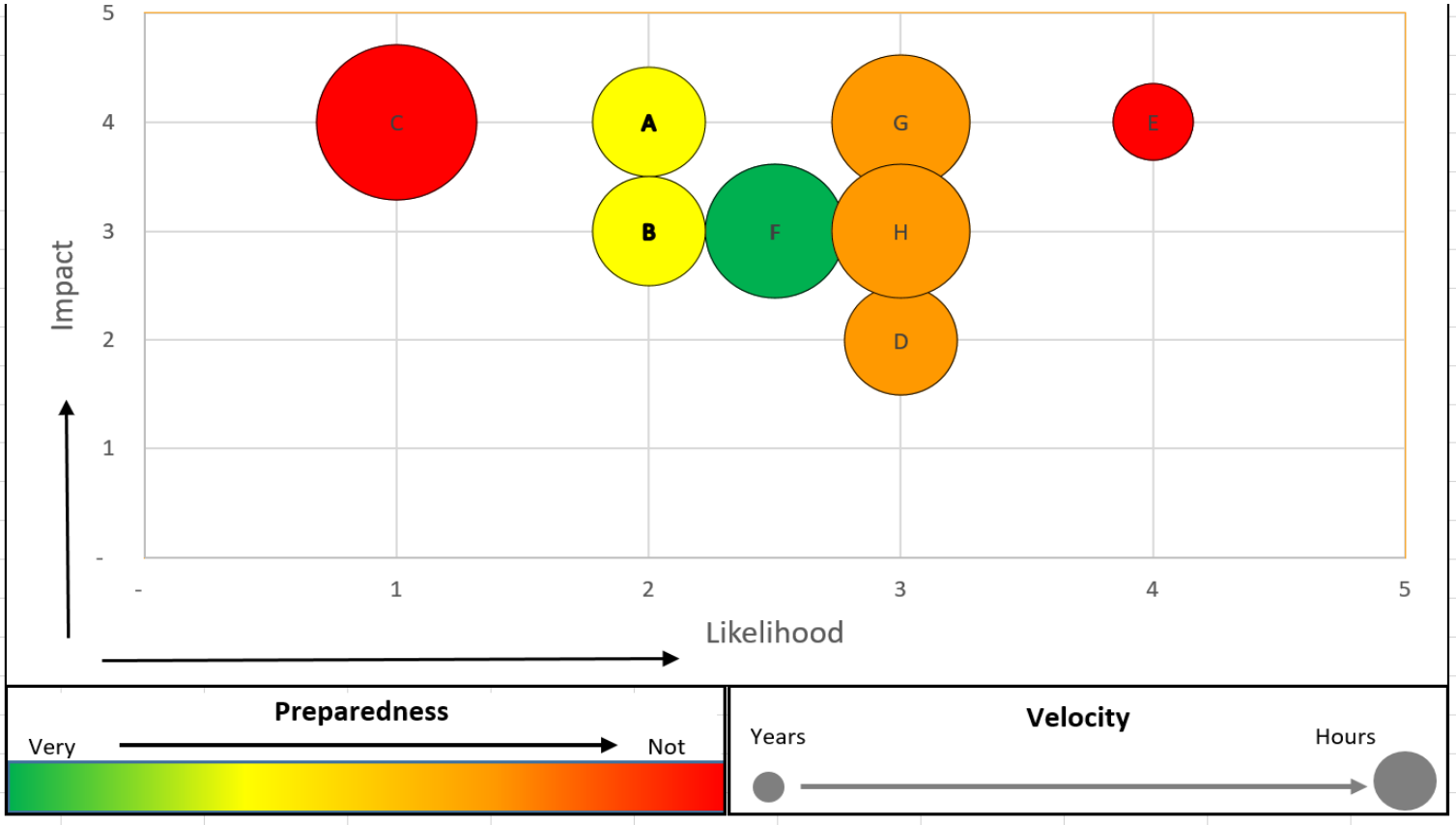
Velocity refers to how quickly a risk could impact the organization.

Preparedness refers to the organization's readiness to deal with a risk and might include the existence and effectiveness of such aspects as prevention or detection controls, recovery arrangements, backups, response plans, communication plans, etc.

Reporting Guidelines

- November 1st – TTUSA Office of Risk Management (ORM) initiates update process with component institutions
- April 1st – Component institution updates due to ORM
  - Risk management review for System wide common risks
  - Clarify, as needed, with component
- May Board meeting – TTUSA and components presentations

Attachment: Major Risk Category Heat Map



Attachment: Rating Scales

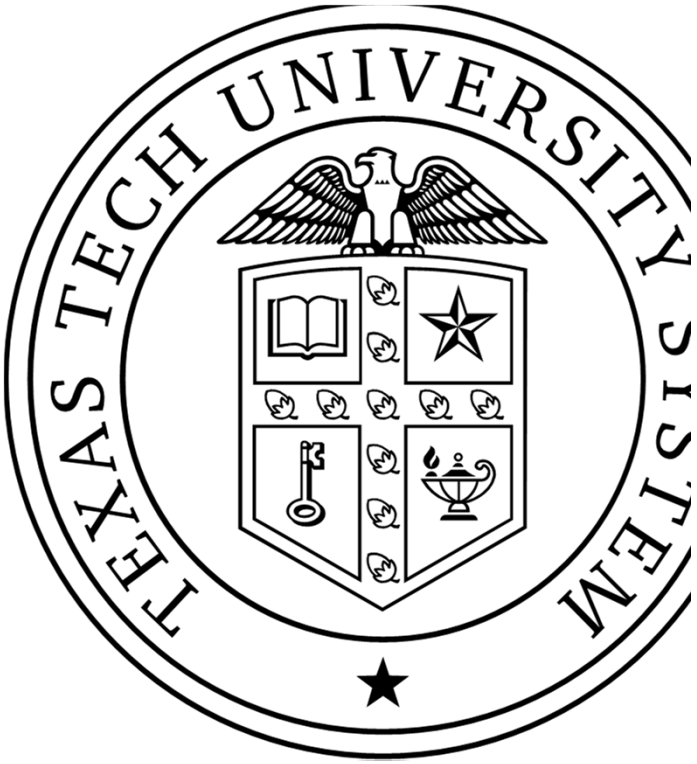
IMPACT					
		Financial	Operational	Compliance	Strategic
Level		Resources, financial structure, ability to meet future financial needs, financial reporting	Continuity of activities, safety and security, IT operations, physical infrastructure, process efficiency, program effectiveness	Legal, regulatory, 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.

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.

Questions?



TEXAS TECH UNIVERSITY SYSTEM™