Texas Tech University System

Enterprise Risk Management Workshop

October 31, 2017

ERM Overview
Evolution of Risk Management

Risk

Traditional Definition

The possibility that something bad or unpleasant will happen.

Merriam-Webster

Minimizing the adverse effects of accidental losses.

The Institutes

Risk

Broadened Definition

The effect of uncertainty on objectives.

ISO 31000

Coordinated activities to direct and control an organization with regard to risk.

ISO 31000

Why is Risk Management Important?

1.

All organizations exist to achieve their objectives.

2.

Many internal and external factors affect those objectives, causing uncertainty about whether the organization will achieve its objectives.

3.

The effect this uncertainty has on an organization's objectives is "risk."

In summary, the management of risk is central to the livelihood and success of all organizations.

The *New View* of Risk

RISK can be a threat or opportunity

Anything that can harm, prevent, delay, *or enhance* an organization's ability to achieve objectives = RISK

The *New View* of Risk

The Changing Focus of Risk Management

Strategic

Integrated

Transactional

Enterprise-Wide Risk Management
- Broad range of risks analyzed
- Combination of risk controls & opportunities
- ERM alignment with strategy
- Helps manage growth, allocate capital & resources
- Risks owned by SME's
- Greater availability of risk mitigation and analytical tools
- Risk Manager = risk moderator, partner, leader; *not* the owner of every risk

Advanced Risk Management
- Alternative risk transfer techniques
- Proactive prevention & risk reduction
- Integrated approach to claims, contracts, insurance, etc.
- Increased education & accountability
- Collaboration across departments
- Risk Manager *may* be the risk owner

Historic Risk Management
- Insurance
- Specific hazards
- No compliance input
- Separate safety & emergency management
- "Silo" approach
- Risk Manager = insurance buyer

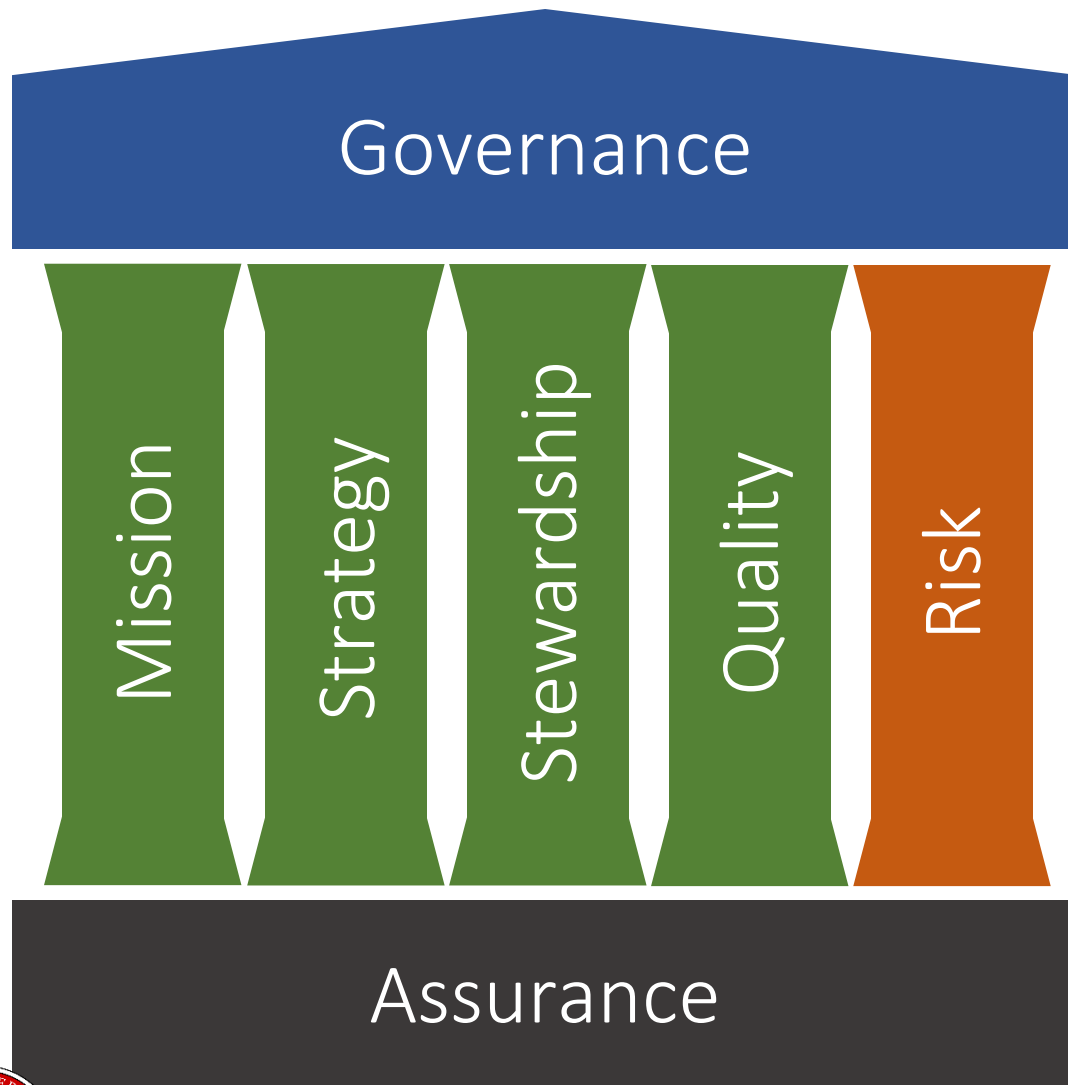|		
Risk is bad – focus is on transferring risk	**Risk is an expense – focus is on reducing cost-of-risk**	**Risk is uncertainty – focus is on optimizing risk to achieve goals**

ERM Overview

Importance of ERM in governance

Risk Management as an Integral Pillar of Governance

Assurance

A strong management structure and culture is maintained to ensure proper reporting and accountability, and internal and external audits are utilized to bring board assurance.

Centralized Oversight-Decentralized Implementation

		Oversight	
		Centralized	**Decentralized**
Implementation	**Centralized**	Where some have developed, but centralized implementation requires significant staff and does not take advantage of current subject matter expertise	
	Decentralized	Oversight is at highest levels, including board, but implementation is pushed out to experienced subject matter experts through risk "ownership"	Where most entities have been, although with some limited departmental oversight, but does not incorporate board-level reporting and accountability

Who is Interested in Enterprise Risk Management?

External
Stakeholders

Board   Community
Senior Leaders   Government
Faculty   Vendors
Staff   Creditors
Affiliates   Rating Agencies
Alumni   Accrediting Bodies

ERM Overview
How does ERM impact strategy?

Case for Enterprise Risk Management

"When we first began our URM (University Risk Management) program in 2013, I could not have imagined the **value proposition** that was about to transcend our institution. What started out as mostly defensive and guarded discussions of threats and barriers to achieving the University mission, quickly and completely turned around into a **robust conversation about opportunities and strategic planning**. Our senior-level risk committee meetings are lively and well-represented. It is amazing how our cross-functional committee, while staying focused on our risk and compliance-based decisioning model, is **driving real innovation and progress** throughout the University."

Doug Huffner, J.D.
Senior Director and Chief Risk Officer
The Ohio State University

What Makes ERM Work?

Focuses on mission and objectives

Preserves and creates value

Emboldens innovation

Enhances agility and resilience

Formalizes process and governance

Improves quality of decisions

Helps in allocation of resources

Empowers subject matter experts

Improves stakeholder confidence and trust

ERM Overview
The importance of senior leaders

Role of Senior Leaders

- Support & Commitment
- Tone at the Top
- Board Reporting
- Build in Accountability
- Risk-Aware Culture
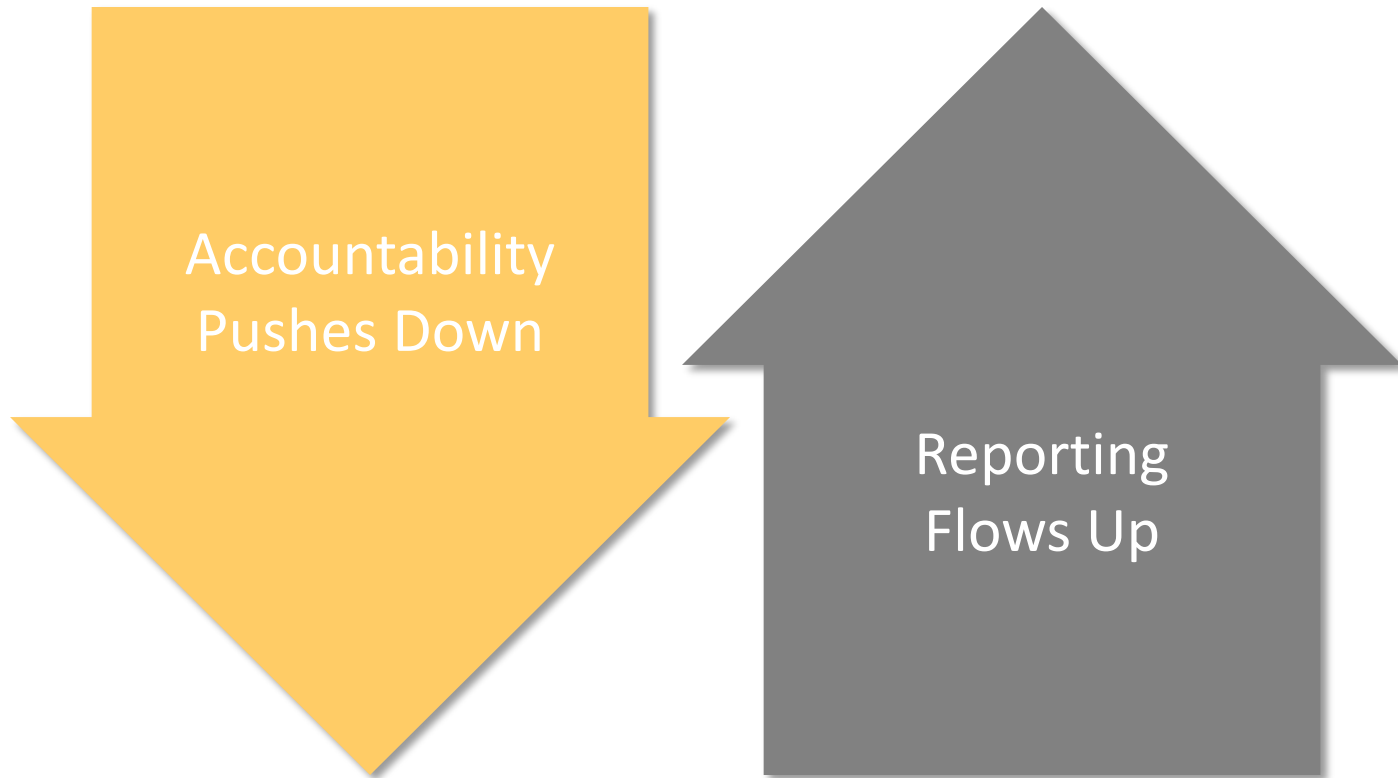- Continual Improvement

Integrated into Existing Business Practices

- Not new functions

- Incorporated into:

    - Strategic Planning

    - Quality Improvement

    - Budgeting

    - Employee Engagement

    - Committee Structure

    - Decision-Making

    - …..

Reporting & Accountability Clearly Addressed

Accountability
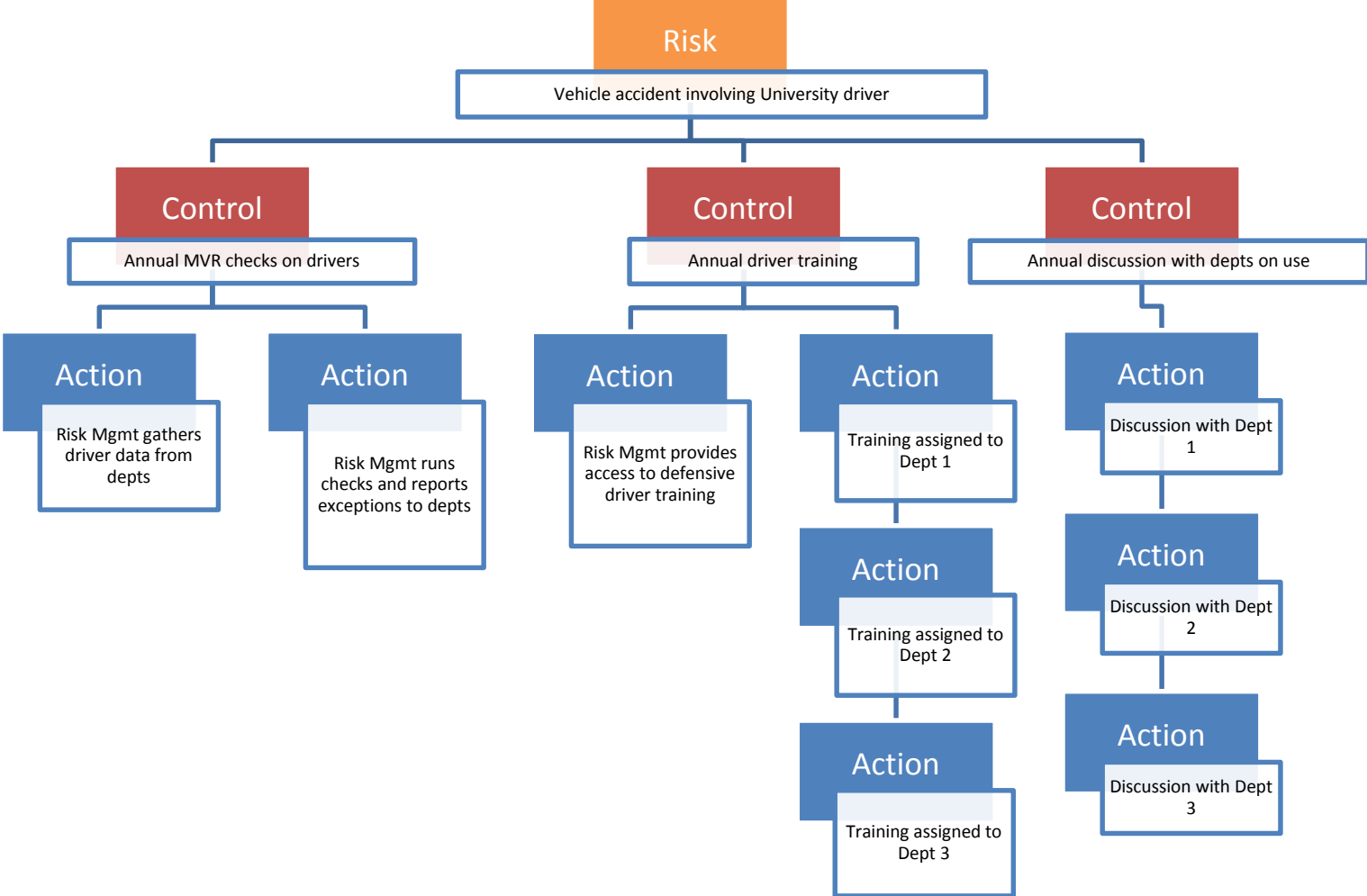Pushes Down

Reporting
Flows Up

Embracing the "Ownership" Model

- Identifying subject matter experts is essential to success

- Risk owners:

  - Develop risk treatment plans

  - Assemble work teams

  - Communicate and report

  - Monitor and evaluate

- At what level of the organization should ownership reside?

  - Based on risk, institutional culture, and where in process maturity

Risk-Control-Action Hierarchy

Risk
Vehicle accident involving University driver

Control
Annual MVR checks on drivers

Control
Annual driver training

Control
Annual discussion with depts on use

Action
Risk Mgmt gathers driver data from depts

Action
Risk Mgmt runs checks and reports exceptions to depts

Action
Risk Mgmt provides access to defensive driver training

Action
Training assigned to Dept 1

Action
Training assigned to Dept 2

Action
Training assigned to Dept 3

Action
Discussion with Dept 1

Action
Discussion with Dept 2

Action
Discussion with Dept 3

Accountability Strategies

- Committees
  - ERM committee
  - Senior leaders
  - Board audit committee
- Governing board reports
- Build into annual cycles
  - Budgeting
  - Planning
- ERM system
  - Workflow management

Three Levels of Risk to Consider

Strategic

Operational

Decision-Making

Where is TTUS ERM Program Now?
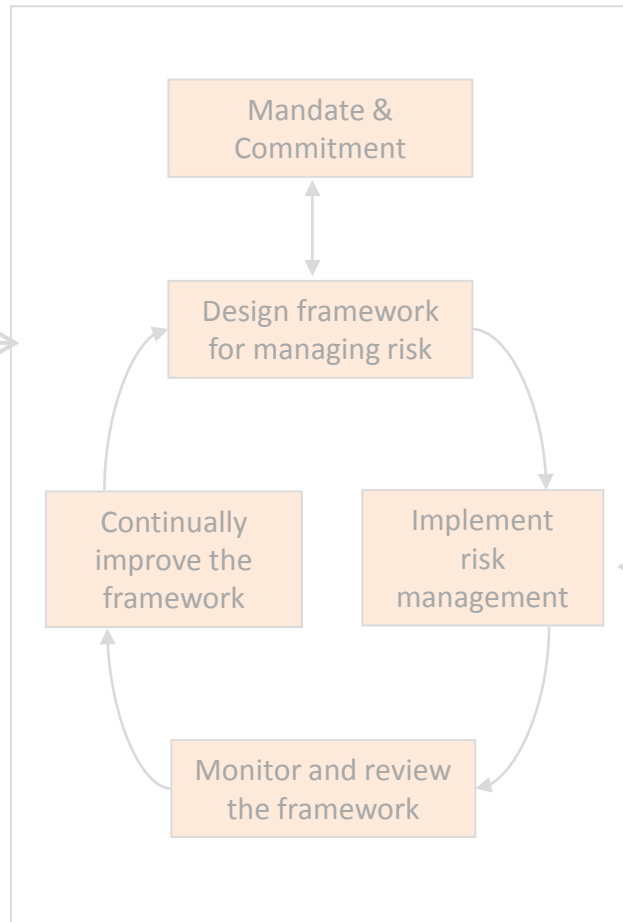## Introduction of Risk Maturity Models
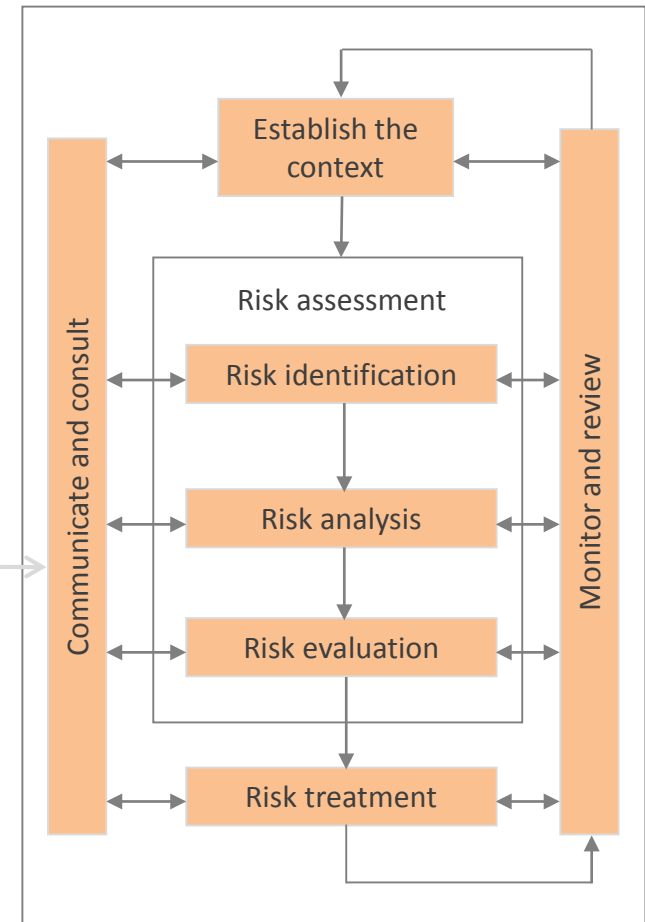
ISO 31000 Risk Management Model

Principles

- Creates value
- Integral part of organizational processes
- Part of decision making
- Explicitly addresses uncertainty
- Systematic, structured and timely
- Based on best available information
- Tailored
- Takes human and cultural factors into account
- Transparent and inclusive
- Dynamic, iterative and responsive to change
- Facilitates continual improvement and enhancement of the organization

Framework

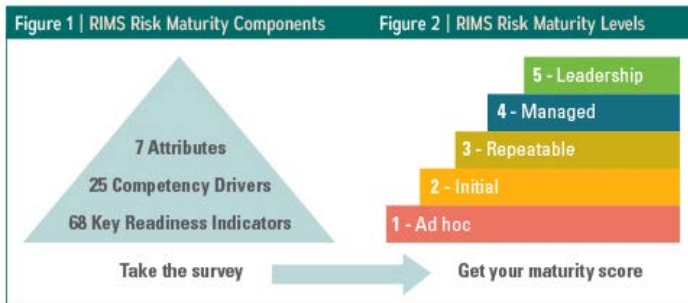Mandate & Commitment

Design framework for managing risk

Continually improve the framework

Implement risk management

Monitor and review the framework

Process

Establish the context

Risk assessment

Risk identification

Risk analysis

Risk evaluation

Risk treatment

Communicate and consult

Monitor and review

ISO 31000 Ten Framework Design Elements

ISO Framework Design Element	Description and Potential Value to the Organization
Understand the Organization & Its Context	Evaluates the culture of the organization as well as articulating trends in the political, regulatory, economic and competitive environment. It considers external stakeholders and their relative importance to the success of the organization, and it looks closely at internal governance, organizational structure, roles of key staff, capital, processes and systems.
Establish Risk Management Policy	ISO recommends a written risk management policy which states the organization's objectives for, and commitment to, risk management and addresses the role of risk management as a means of increasing the likelihood of meeting objectives, accountability and responsibility for managing risk, commitment of necessary resources, measurement and reporting, and agreement for review and improvement of the process over time.
Accountability	Accountability and authority should be established for the implementation and maintenance of the risk management process and ensuring the adequacy, effectiveness and efficiency of controls. This accountability can be facilitated by identifying risk owners with adequate authority to treat particular risks, identifying those responsible for maintaining and improving the framework, identifying responsibilities for all employees and at all levels, establishing performance measurement, and setting procedures for internal and external reporting.
Integration into Organizational Processes	Embedding risk management into all of the organization's practices and processes in a way that is relevant, effective and efficient is crucial to creating a lasting ERM culture. It should become part of, and not separate from, organizational processes such as business and strategic planning, policy development, change management, quality improvement, compliance, budgeting, and employee evaluation.
Resources	The organization should allocate sufficient resources to support the risk management process. Consideration should be given to the people, skills, experience and competence of staff or outside resources, the organization's processes and tools for managing risk, available information and knowledge management systems, and any needed training.
Establish Internal Communication & Reporting	Internal communication and reporting is crucial to the successful implementation of ERM. The organization should make sure there are clear reporting mechanisms in place to support and encourage accountability and risk ownership. These mechanisms should ensure that key components of the risk management framework are communicated throughout the organization, effectiveness and outcomes are highlighted, and processes are in place to consolidate risk information from a variety of sources taking into account the sensitivity of some data.
Establish External Communication & Reporting	The organization should develop a plan for how it will communicate with outside stakeholders. This should involve engaging appropriate external stakeholders and ensuring an effective exchange of information, compliance with various legal, regulatory and governance requirements, and developing a plan for communicating externally in the event of a crisis. As with internal communications, processes should be established to consolidate risk information and take into account the sensitivity of some data.
Implementation	Implementation should be considered at two levels. The first is the implementation of the framework itself. This is accomplished by defining the appropriate strategy and timing for establishing the framework within the organization, applying the risk management policy to the organization's established business processes, and ensuring that risk management is clearly part of decision making, including the development of objectives. The second level is the implementation of the risk management process at all relevant levels and functions of the organization as part of its processes and practices.
Monitor & Review	The framework should be reviewed periodically to ensure that risk management is effective and continues to support organizational performance. The review should consider the measurement of risk management performance against indicators along with the periodic review of those indicators, measurement of progress against the risk management plan, and review of whether the framework, policy and plan are still appropriate and effective given the organization's internal and external context.
Continuous Improvement	Based on the results of the monitoring and review, decisions should be made on how the framework, policy and plan can be improved. These decisions should lead to actionable items for the improvement of the management of risk and greater infiltration of ERM processes and principles into the organizational culture.

RIMS Risk Maturity Model

Figure 1 | RIMS Risk Maturity Components

7 Attributes
25 Competency Drivers
68 Key Readiness Indicators

Take the survey → Get your maturity score

Figure 2 | RIMS Risk Maturity Levels

5 - Leadership
4 - Managed
3 - Repeatable
2 - Initial
1 - Ad hoc

Attributes	Maturity Levels					
	Level 5: Leadership	Level 4: Managed	Level 3: Repeatable	Level 2: Initial	Level 1: Ad hoc	Nonexistent
1 Adoption of ERM-based approach	Key Drivers: Degree of … • support from senior management, Chief Risk Officer • business process definition determining risk ownership • assimilation into support area and front-office activities • far-sighted orientation toward risk management • risk culture's accountability, communication and pervasiveness					
2 ERM process management	Key Drivers: Degree of … • each ERM Process step (see definition) • ERM Process's repeatability and scalability • ERM Process oversight including roles and responsibilities • risk management reporting • qualitative and quantitative measurement					
3 Risk appetite management	Key Drivers: Degree of … • risk-reward tradeoffs • risk-reward-based resource allocation • analysis as risk portfolio collections to balance risk positions					
4 Root cause discipline	Key Drivers: Degree of … • classification to manage risk and performance indicators • flexibility to collect risk and opportunity information • understanding dependencies and consequences • consideration of people, relationships, external, process and systems views					
5 Uncovering risks	Key Drivers: Degree of … • risk ownership by business areas • formalization of risk indicators and measures • reporting on follow-up activities • transforming potentially adverse events into opportunities					
6 Performance management	Key Drivers: Degree of … • ERM information integrated within planning • communication of goals and measures • examination of financial, customer, business process and learning • ERM process goals and activities					
7 Business resiliency and sustainability	Key Drivers: Degree of … • integration of ERM within operational planning • understanding of consequences of action or inaction • planning based on scenario analysis					

Value of Risk Maturity Models

- Helps determine next steps
  - Rest of current year
  - 2-5 year horizon
- Provides common language of risk with external stakeholders
  - Rating agencies
  - Accrediting bodies
  - Government

Where is TTUS ERM Program Now?
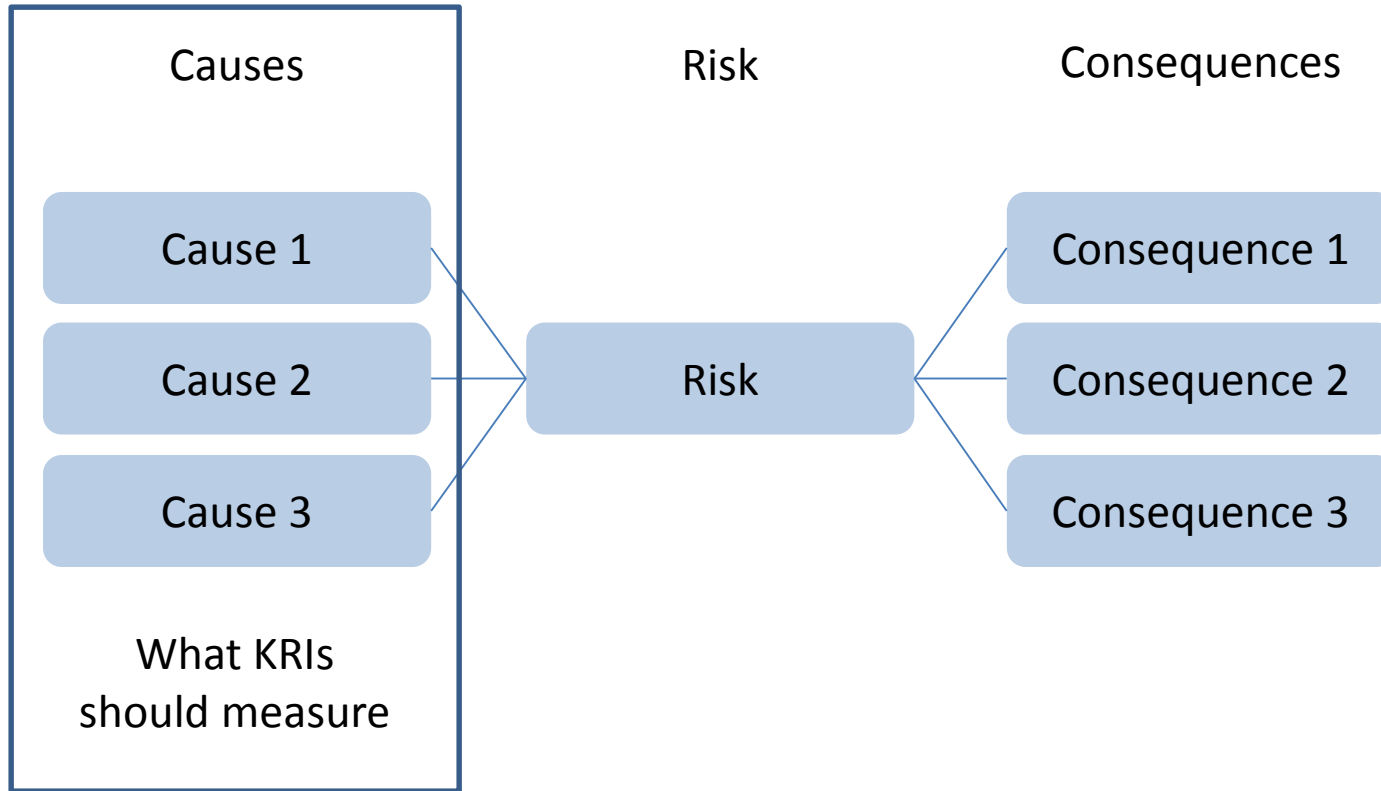## Use of Key Risk Indicators (KRIs)

KRI Definition

- *KRIs are metrics used to provide an early signal of increasing risk exposure in various areas of the organization.*

  - NC State Poole College of Management, Enterprise Risk Management Initiative

- Differs from KPIs:

  - KPI measures how well something is being done in pursuit of mission and objectives

  - KRI is an early warning for events that could harm the mission and objectives

- What makes a well-constructed KRI?

  - Starts with *Root Cause* or *Bowtie* Analysis

  - Proper linking of KRIs to risks
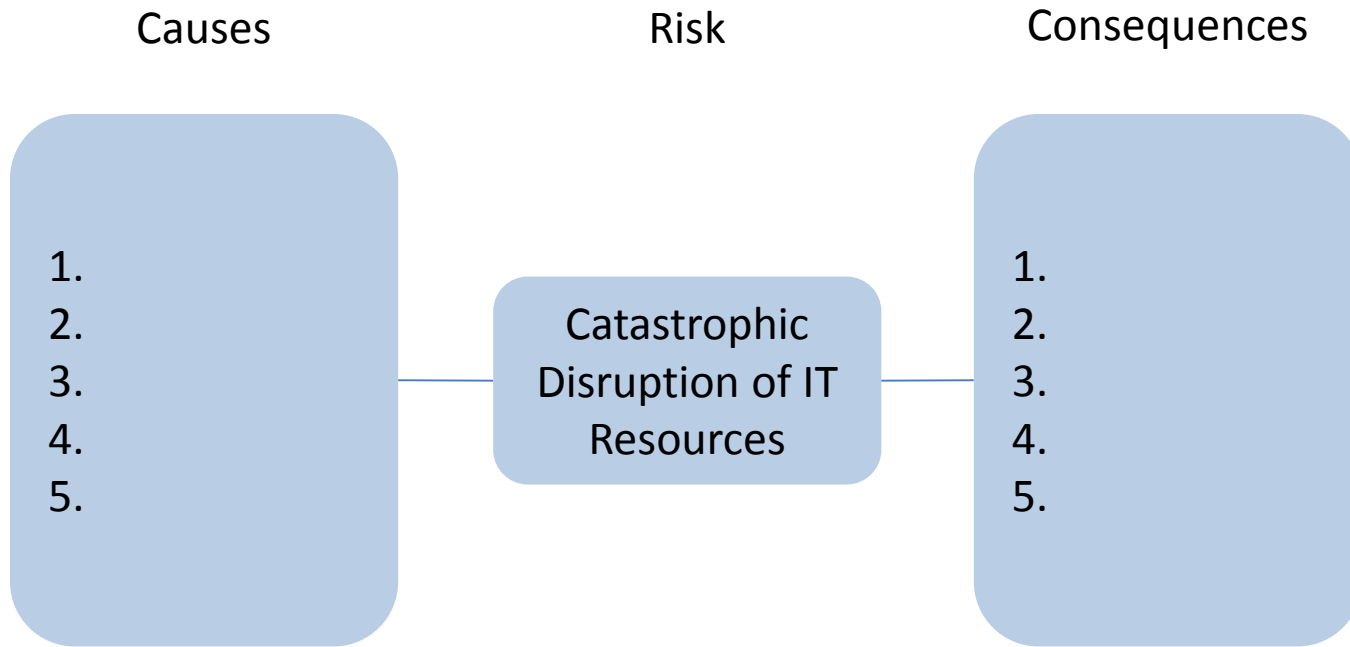
  - Quantifiable and measurable

  NOTE: Not all risks will have KRIs and some risks may have several

Bowtie Analysis

Causes   Risk   Consequences

Cause 1   Risk   Consequence 1

Cause 2   Consequence 2

Cause 3   Consequence 3

What KRIs should measure

Exercise

Causes

Risk

Consequences

1.
2.
3.
4.
5.

Catastrophic
Disruption of IT
Resources

1.
2.
3.
4.
5.

Exercise

Causes

1.
2.
3.
4.
5.

KRIs

1.
2.
3.
4.
5.

Where is TTUS ERM Program Now?
How will we measure success/progress?

2017 Top Identified Risk Themes

Financial	• Revenue, uncertainty of State appropriations, tuition freeze, federal dollars for research & student financial aid, philanthropy, investment returns
Campus Safety, Health & Security	• Title IX, terrorist threat, train derailment, weather
Information Technology	• Cybersecurity, increase network infrastructure resiliency, employee training & awareness
Compliance	• Federal and State statutes/regulations, research, bond covenants
Accreditation	• Compliance with SACSCOS standards & criteria, seeking & maintaining college/program specific accreditation
Enrollment Management	• Enrollment forecasting, retention, graduation rates, revenue modeling, faculty hires
Retention/Hiring Faculty & Staff	• Ability to attract & retain renowned faculty & qualified staff
Continuity of Operations	• Compliance with State law, where & how to continue business/academic operations following major incident, exercised plans system wide

Enterprise Risk Management Workshop

Texas Tech University System

Enterprise Risk Management Workshop