TEXAS TECH UNIVERSITY SYSTEM™

Enterprise Risk Management Report

Penny Harkey
Interim Vice Chancellor & Chief Financial Officer
Kim Turner
Chief Audit Executive

May 5, 2022

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 considers risk at the enterprise level and is a powerful tool in strategic planning, resource allocation, risk management and audit planning.

- ERM philosophy is to focus on key elements to serve as a management and communication tool that assists in reducing risks and improving chances of success in accomplishment of goals found in strategic plan and/or other key continuing operational programs.

ERM Process

- Introduced in Spring 2016
- ***System Regulation 1.1.1*** formalizes ERM framework and establishes recurring timeline for completing/reporting to Board.
- All levels of management are involved in identifying and managing risk at an enterprise level vs. in siloes.
- Risk Management is continual and ongoing. Not limited to a periodic report.
- TTUS Office of Risk Management provides guidance and templates reporting.

Key Elements of ERM Framework

Identify and Prioritize Risk

- Identify and prioritize risk associated with the achievement of strategic plan goals and/or other key continuing operational programs.

Determine Level of Acceptable Risk

- Management and the board determines acceptable levels of risk, including acceptance of risks designed to accomplish the organization's objectives.

Develop Mitigation Activities

- Develop and implement mitigation activities to reduce risk or risk impact.

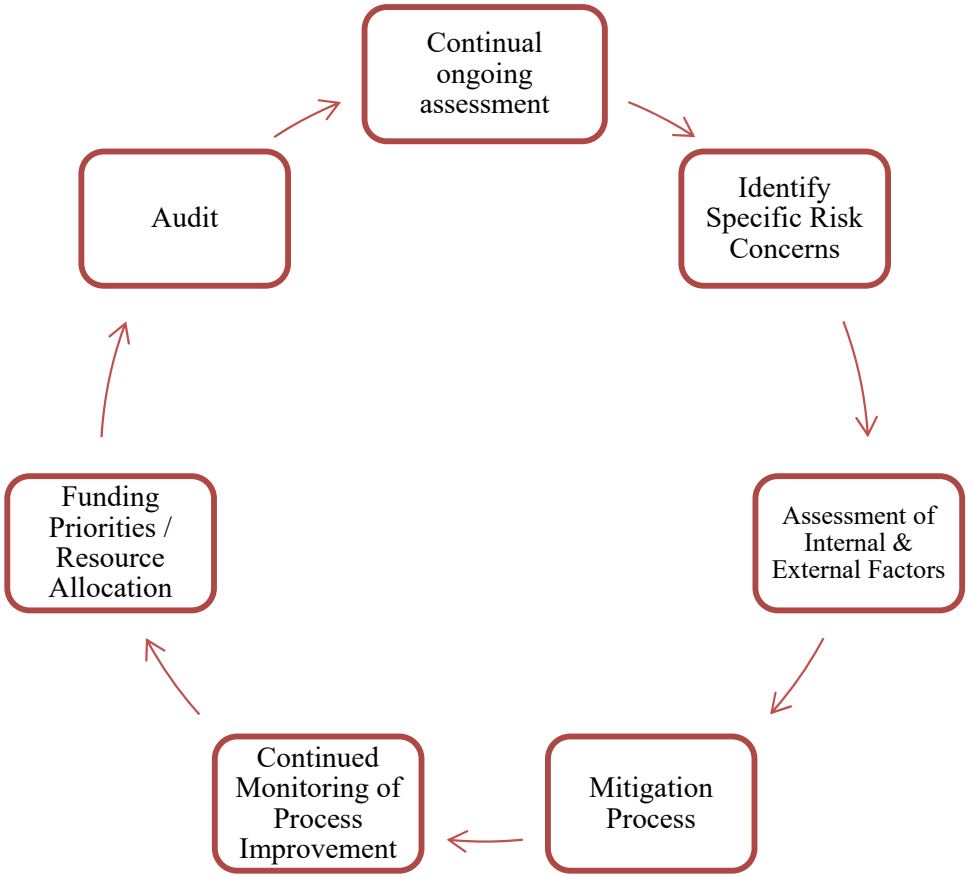
Conduct Ongoing Monitoring

- Conduct monitoring activities to periodically reassess risk and the effectiveness of controls to manage risk.

Report Periodically on ERM Process

- Report and communicate periodically on the application of the ERM tools in the management of risk. Risk deficiencies should be reported upstream, with serious matters reported to top management and the board.

ERM Process


Continual ongoing assessment
Identify Specific Risk Concerns
Assessment of Internal & External Factors
Mitigation Process
Continued Monitoring of Process Improvement
Funding Priorities / Resource Allocation
Audit

ERM Risk Types

Financial	Operational	Information Technology	Compliance	Strategic
• Resources • Enrollment • Inflation • Financial structure • Ability to meet future financial needs • Financial reporting	• Continuity of activities • Safety and security • Physical infrastructure • Process efficiency • Program effectiveness • Recruitment and retention	• IT strategy and operations • Data breach • Cybersecurity • IT upgrades and infrastructure	• Legal • Regulatory (state and federal) • Contractual • Accreditation standards • NCAA • Data privacy	• Organizational reputation • Constituent relationships • Ability to generate funds • Strategic priorities

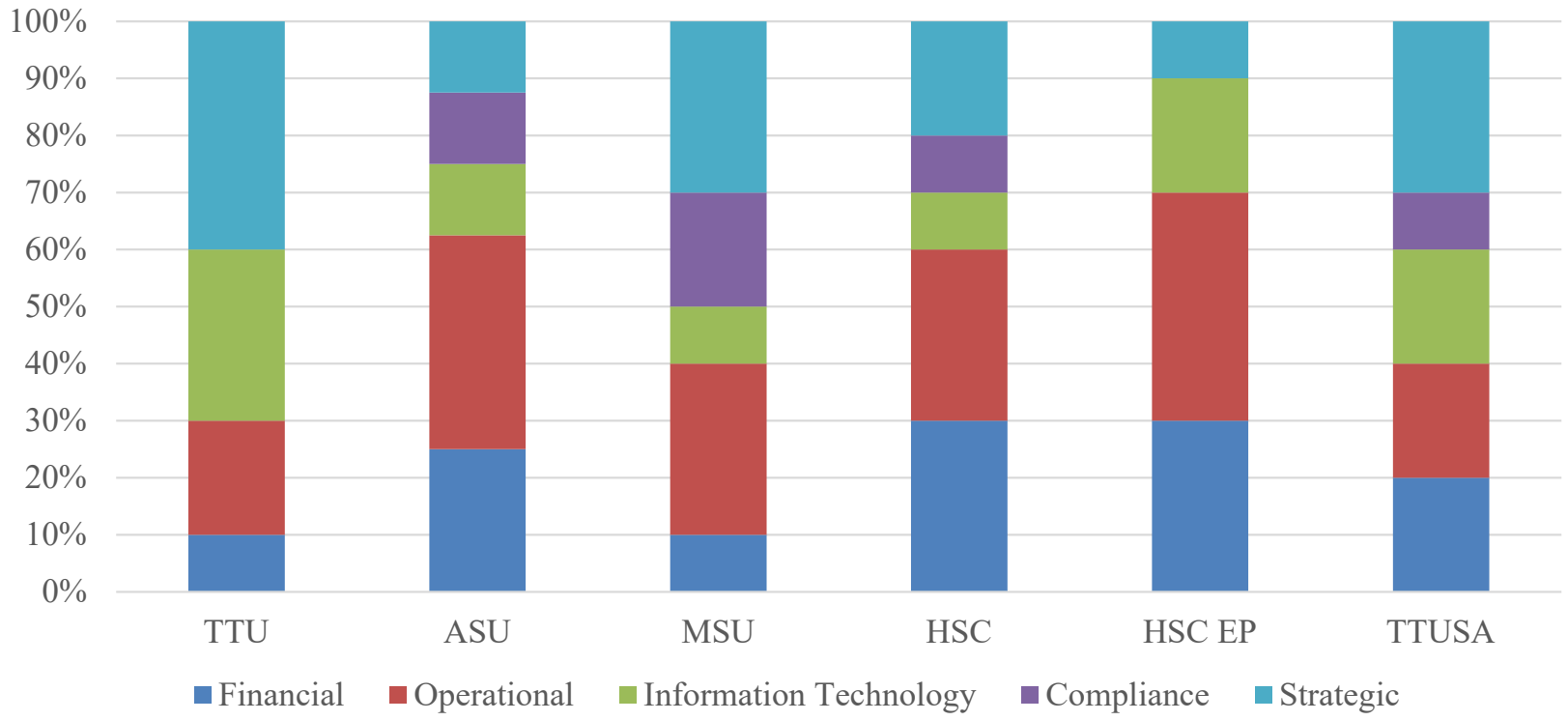
2022 TTUS ERM

Risk Levels, Defined by Category

Risk Levels	Financial	Operational	Information Technology	Compliance	Strategic
Minor	Insignificant financial impact.	Negligible interruption to activities. Negligible effect on efficiency and effectiveness.	Minor information technology event. No loss of infrastructure.	Minor incidental compliance violations.	No discernable negative impact to reputation and/or goal achievement. Minor media coverage. Negative effect on constituent satisfaction or relationships.
Moderate	Notable financial impact.	Brief or limited interruption of activities. Moderate loss of process efficiency and/or program effectiveness.	Notable information technology event. Minor loss of infrastructure.	Repetitive or systemic compliance violations.	Notable temporary negative impact to reputation and/or goal achievement. Some media coverage. Constituent dissatisfaction or strain on relationships.
Major	Material financial impact.	Major interruption of activities. Moderate safety or security concerns.	Major information technology event. Localized loss of infrastructure.	Major compliance violations.	Major negative impact to reputation and/or goal achievement. National media coverage. Constituent dissatisfaction and loss of relationships.
Severe	Financial impact threatens solvency or ability to continue operations.	Extensive interruption of activities. Significant safety or security concerns.	Significant information technology event. Significant loss of infrastructure.	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.

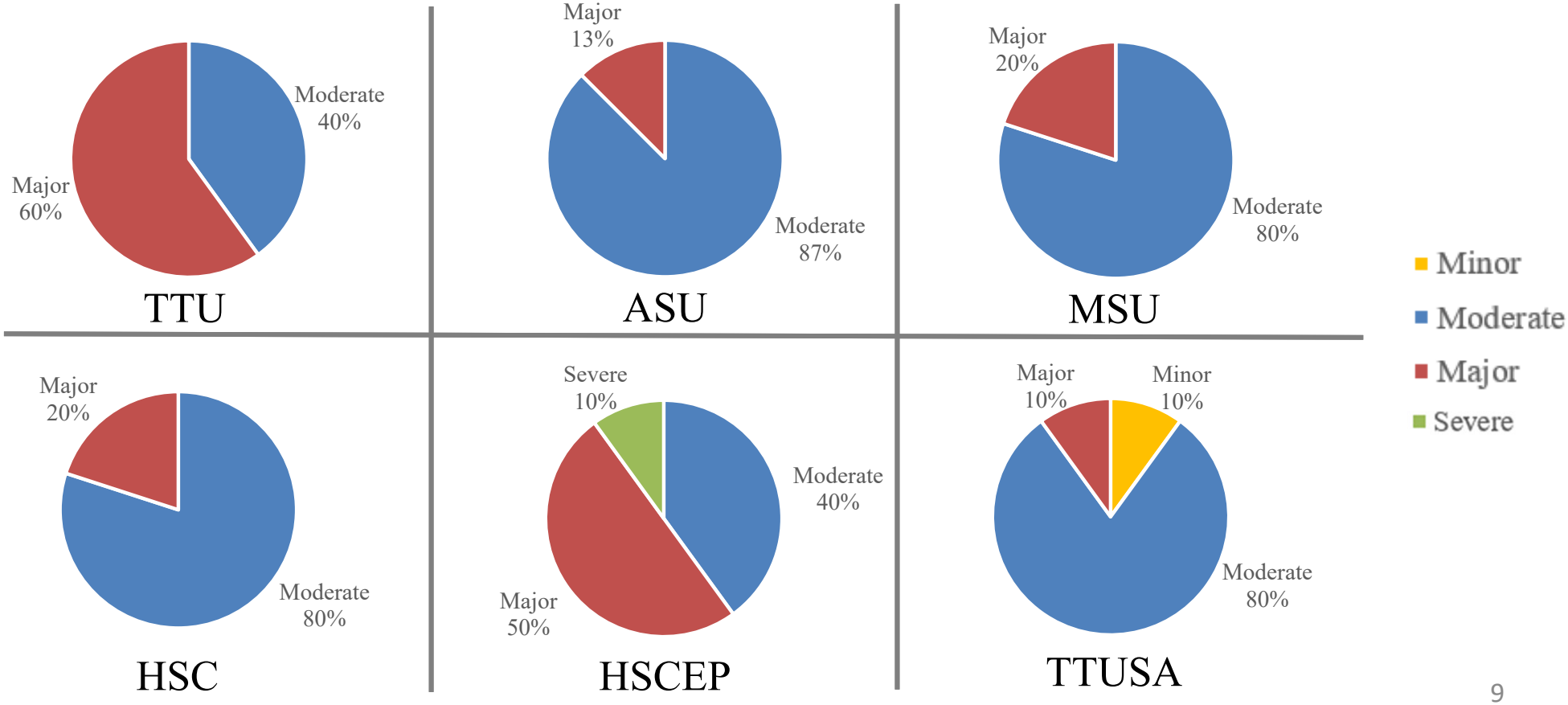
2022 TTUS ERM

Risk Categories by Component



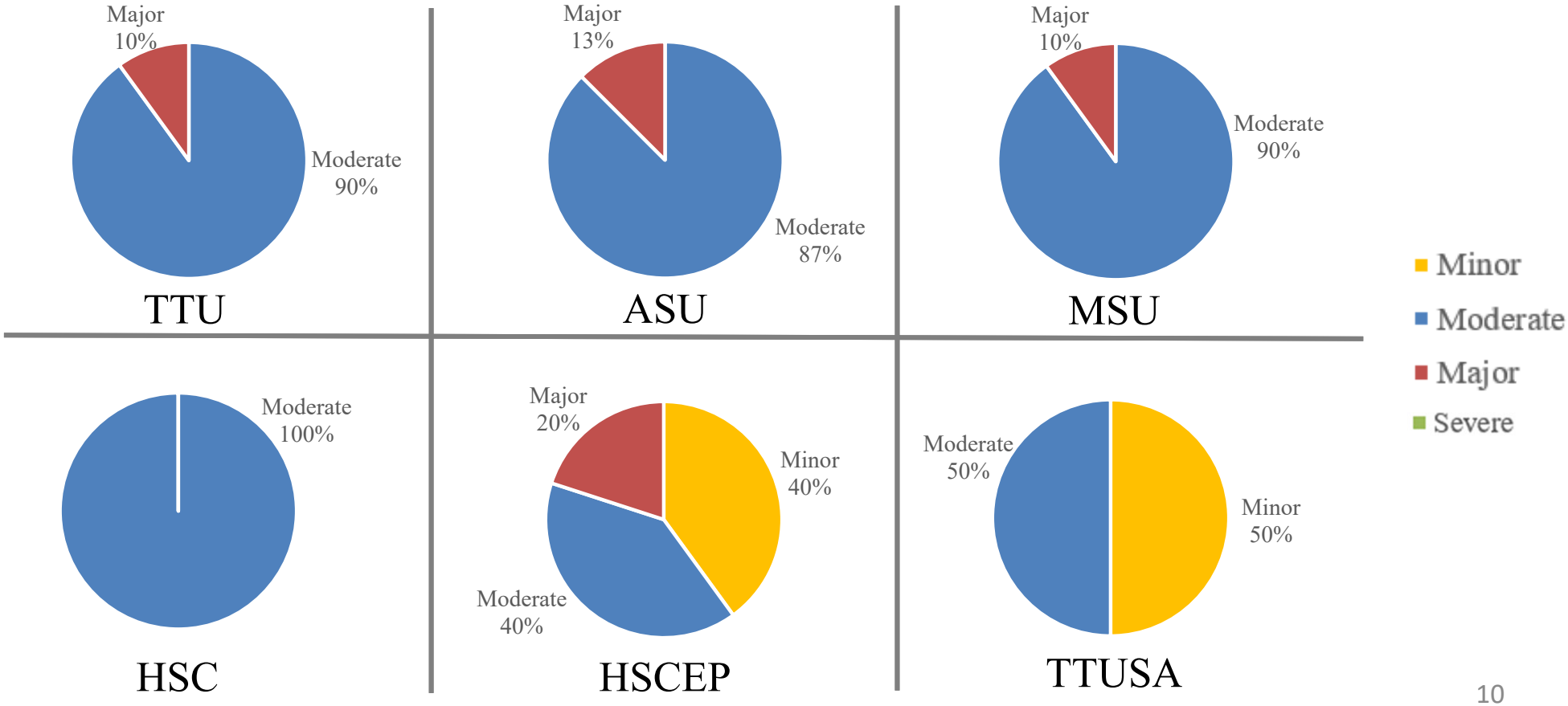
2022 TTUS ERM

Risk Breakdown by Risk Type without Mitigation Strategies



2022 TTUS ERM

Risk Breakdown by Risk Type with Mitigation Strategies



2022 TTUS ERM Reporting Examples

Financial	• State and federal funding • Inflation
Operational	• Employee recruitment and retention • Weather, energy and environmental impacts
Information Technology	• Cybersecurity breach • Data security
Compliance	• New and changing regulatory requirements • Conflicts of interest management
Strategic	• Institutional and programmatic accreditation • Reputational risk