Enterprise Risk Management Report

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

May 5, 2022
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
- Audit
- Identify Specific Risk Concerns
- Funding Priorities / Resource Allocation
- Assessment of Internal & External Factors
- Continued Monitoring of Process Improvement
- Mitigation Process
## ERM Risk Types

<table>
<thead>
<tr>
<th>Financial</th>
<th>Operational</th>
<th>Information Technology</th>
<th>Compliance</th>
<th>Strategic</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Resources</td>
<td>• Continuity of activities</td>
<td>• IT strategy and operations</td>
<td>• Legal</td>
<td>• Organizational reputation</td>
</tr>
<tr>
<td>• Enrollment</td>
<td>• Safety and security</td>
<td>• Data breach</td>
<td>• Regulatory (state and federal)</td>
<td>• Constituent relationships</td>
</tr>
<tr>
<td>• Inflation</td>
<td>• Physical infrastructure</td>
<td>• Cybersecurity</td>
<td>• Contractual</td>
<td>• Ability to generate funds</td>
</tr>
<tr>
<td>• Financial structure</td>
<td>• Process efficiency</td>
<td>• IT upgrades and infrastructure</td>
<td>• Accreditation standards</td>
<td>• Strategic priorities</td>
</tr>
<tr>
<td>• Ability to meet future financial needs</td>
<td>• Program effectiveness</td>
<td></td>
<td>• NCAA</td>
<td></td>
</tr>
<tr>
<td>• Financial reporting</td>
<td>• Recruitment and retention</td>
<td></td>
<td>• Data privacy</td>
<td></td>
</tr>
</tbody>
</table>
## 2022 TTUS ERM
### Risk Levels, Defined by Category

<table>
<thead>
<tr>
<th>Risk Levels</th>
<th>Financial</th>
<th>Operational</th>
<th>Information Technology</th>
<th>Compliance</th>
<th>Strategic</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Minor</strong></td>
<td>Insufficient financial impact.</td>
<td>Negligible interruption to activities. Negligible effect on efficiency and effectiveness.</td>
<td>Minor information technology event. No loss of infrastructure.</td>
<td>Minor incidental compliance violations.</td>
<td>No discernable negative impact to reputation and/or goal achievement. Minor media coverage. Negative effect on constituent satisfaction or relationships.</td>
</tr>
<tr>
<td><strong>Moderate</strong></td>
<td>Notable financial impact.</td>
<td>Brief or limited interruption of activities. Moderate loss of process efficiency and/or program effectiveness.</td>
<td>Notable information technology event. Minor loss of infrastructure.</td>
<td>Repetitive or systemic compliance violations.</td>
<td>Notable temporary negative impact to reputation and/or goal achievement. Some media coverage. Constituent dissatisfaction or strain on relationships.</td>
</tr>
<tr>
<td><strong>Severe</strong></td>
<td>Financial impact threatens solvency or ability to continue operations.</td>
<td>Extensive interruption of activities. Significant safety or security concerns.</td>
<td>Significant information technology event. Significant loss of infrastructure.</td>
<td>Significant, chronic, and/or pervasive compliance violations.</td>
<td>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.</td>
</tr>
</tbody>
</table>
2022 TTUS ERM
Risk Categories by Component

TTU ASU MSU HSC HSC EP TTUSA

Financial   Operational   Information Technology   Compliance   Strategic
2022 TTUS ERM
Risk Breakdown by Risk Type without Mitigation Strategies

TTU

ASU

MSU

HSC

HSCEP

TTUSA

- TTU: Major 60%, Moderate 40%
- ASU: Major 13%, Moderate 87%
- MSU: Major 20%, Moderate 80%
- HSC: Major 20%, Moderate 80%
- HSCEP: Severe 10%, Moderate 40%, Major 50%
- TTUSA: Major 10%, Minor 10%, Moderate 80%
2022 TTUS ERM
Risk Breakdown by Risk Type with Mitigation Strategies

TTU:
- Major: 10%
- Moderate: 90%

ASU:
- Major: 13%
- Moderate: 87%

MSU:
- Major: 10%
- Moderate: 90%

HSC:
- Major: 100%

HSCEP:
- Major: 20%
- Moderate: 40%
- Minor: 40%

TTUSA:
- Moderate: 50%
- Minor: 50%
### 2022 TTUS ERM Reporting Examples

<table>
<thead>
<tr>
<th>Category</th>
<th>Examples</th>
</tr>
</thead>
</table>
| 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                                                        |