Standard & Poor's ERM Quality Classifications

<table>
<thead>
<tr>
<th></th>
<th>Excellent</th>
<th>Strong</th>
<th>Adequate</th>
<th>Weak</th>
<th>Weak</th>
<th>[Nonexistent]</th>
</tr>
</thead>
</table>
| Excellent      | • Advanced capabilities to identify, measure, manage all risk exposures within tolerances  
|                | • Advanced implementation, development and execution of ERM parameters  
|                | • Consistently optimizes risk adjusted returns throughout the organization |
| Strong         | • Clear vision of risk tolerance and overall risk profile  
|                | • Risk Control exceeds adequate for most major risks  
|                | • Has robust processes to identify and prepare for emerging risks  
|                | • Incorporates risk management and decision making to optimize risk adjusted returns |
| Adequate       | • Has fully functioning control systems in place for all of their major risks  
|                | • May lack a robust process for identifying and preparing for emerging risks  
|                | • Performing good classical “silo” based risk management  
|                | • Not fully developed process to optimize risk adjusted returns |
| Weak           | • Incomplete control process for one or more major risks  
|                | • Inconsistent or limited capabilities to identify, measure or manage major risk exposures |

UC Maturity Levels

<table>
<thead>
<tr>
<th></th>
<th>Level 5: Leadership</th>
<th>Level 4: Managed</th>
<th>Level 3: Repeatable</th>
<th>Level 2: Initial</th>
<th>Level 1: Ad hoc</th>
<th>Nonexistent</th>
</tr>
</thead>
</table>

**COSO Elements**

**1. Internal Environment/Objectives Setting**

- **Key Drivers: Degree of...**
  - support by high level leadership for including risk discussion/analysis in campus initiatives  
  - recognition of importance of early risk discussion/analysis related to long-range initiatives among high level leadership  
  - desire and ability of high level leadership to incorporate risk tolerance/management communications and training in daily operations

- **Examples**
  - ERM activities established in ERM Steering Committee or other multidisciplinary committee (Audit, Compliance, Control Groups)  
  - Policy on managing risks  
  - ERM Charter*  
  - ERM Work Plan*  
  - Compliance Officer and Compliance Committee

**2. Event Identification/Risk Assessment**

- **Key Drivers: Degree of...**
  - risk management reporting  
  - qualitative and quantitative measurement  
  - risks are analyzed  
  - risk identified is repeatable and scalable

- **Examples**
  - Risk surveys  
  - Enterprise Risk Assessments*  
  - Audit Reports  
  - Hotline  
  - Strategic/Objective based assessments*  
  - Incident reporting systems  
  - Risk Mapping*  
  - Project Risk Assessments*

* Many referenced documents are available in the ERM Tool Kit: [http://www.ucop.edu/riskmgt/erm/toolkit.html](http://www.ucop.edu/riskmgt/erm/toolkit.html)
| 3. Risk Response/Control Activities | • 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  
• risk ownership by business areas  
• formalization of risk indicators and measures  
• root cause analysis  
• performance management (vision & strategy)  
• Business/Mission resiliency and sustainability | • ERM process reviews  
• Development of KPIs & LIs  
• Retrospective loss reviews  
• Retrospective reviews conducted on losses in >$50,000  
• Risk owners develop risk mitigation plans  
• Balanced Scorecard  
• Internal/External Satisfaction Questions  
• UC Ready Program  
• Be Smart About Safety Program  
• Sustainability Program |
| --- | --- | --- |
| 4. Information and Communication | • reporting on follow-up activities  
• transforming potentially adverse events into educational opportunities  
• communication of goals and measures  
• ERM information integrated with planning  
• education and institutional knowledge | • Websites  
• Newsletters*  
• Training  
• LMS  
• Policy Management Program  
• Written standards of conduct  
• Policies and procedures  
• Learning management Systems (LMS) which track/monitor delivery and frequency of critical training. |
| 5. Monitoring | • ERM process goals and activities  
• understanding of causal relationships between risks and what is measured  
• identification of key metrics to support a risk dashboard  
• alignment of key risk and exposures with monitoring program and processes  
• continuous and stainable risk assessment process to ensure current risk profile and monitoring program  
• automated systems with monitoring capability  
• oversight committee involvement and review  
• compliance and audit functions that attest to all exposures areas, financial and non-finance, in the University | • Metrics development within strategic plans  
• Self-assessments  
• Audits  
• Dashboard providing periodic reporting comprised of metrics aligned with key exposures  
• On-site reviews  
• Automated systems reporting in key compliance areas: e.g. Effort reporting and effort commitment tracking systems, on-line ledger review, etc  
• Regulatory permitting process and requirements: monitoring, record keeping and reporting.  
• SAS 112 certification |

* Many referenced documents are available in the ERM Tool Kit: [http://www.ucop.edu/riskmgmt/erm/toolkit.html](http://www.ucop.edu/riskmgmt/erm/toolkit.html)