Excellence in Risk Management via Enterprise Risk Management

Presentation to: Audit Committee
Ashok K. Roy, Ph.D., CIA, CFSA, CBA
September 18, 2015
We need to migrate to ERM for holistic view of Risks. What is ERM?

Enterprise Risk Management: is “...a process, effected by an entity’s board of directors, management and other personnel, applied in strategy settings and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”*

Notes:
- Several words are highlighted for emphasis: process, strategy, risk appetite, and objectives.
- Risk can be defined as any issue that impacts the University’s ability to meet its objectives.
- Risks cannot be eliminated, but ERM can enable an institution to manage them more efficiently and effectively.

*Committee of Sponsoring Organizations (COSO).
ERM is a superior approach to traditional risk approach

• **Under traditional model/paradigm:** organizations approach risk as a *silo or stovepipe* where certain kinds of risk are pinpointed and then certain executives are charged with managing that risk(s). This often results in silo leaders lobbying a risk or categories of multiple risk to the other silos.

• **Under ERM or new model/paradigm:** organizations try to connect the silos to increase communications between silos to better recognize where one risk may impact multiple silos.
Traditional vs. ERM approaches

**Old/Traditional Paradigm**
- Silo approach
- Focus on insurable risks
- Hazard-based identification and controls

**New/ERM Paradigm**
- Holistic approach
- Wide focus on ALL risks
- Aligns process with strategy, mission
- May include opportunities (upside risks)
Examples of a few Universities who are using ERM approach

- University of California system
- University of Wisconsin system
- University of Colorado system
- Illinois State University
- University of North Carolina – Chapel Hill
- North Carolina State University
- Maricopa County Community College District
- Auburn University
- Penn State University
- University of Denver
- Dartmouth College
- Princeton University
- Lehigh University
The ERM processes in 8 steps

Steps:
- **Setting** the *tone at the top* with Leadership, Culture and Values,
- **Establishing** context, and the basis for how risk is viewed with strategic goals,
- **Identifying** risks, or the harm we are trying to avoid,
- **Assessing** risks using a central focus and common language,
- **Aligning** response options with the level of risk,
- **Documenting** internal controls for top risks,
- **Communicating** with stakeholders and implementing response plans.
- **Monitoring** and measuring to ensure responses have been carried out as intended.
ERM focus is on 4 areas

1. Strategic – high-level goals that are aligned with and support the institution’s mission
2. Operational – ongoing management process
3. Financial – protection of institution's assets
4. Compliance – the institution's adherence to applicable laws and regulations

Reputational risk is often included as a critical higher education risk. However, a serious event in the above listed areas can cause reputational risks. In other words, reputation is always at risk, but not a risk.

Hazard risks (generally covered by insurance, e.g. workers compensation, natural hazards, environmental impairment).
8 Components of ERM cut across 4 areas

For example, there are strategic, operation, reporting, and compliance aspects of the “internal environment.”

1. **Internal environment** – the culture, values, and environment in which an institution operates
2. **Objective setting** – the process that management uses to set its strategic goals and objectives
3. **Event identification** – internal and external events that could affect an institution's ability to achieve its objectives
4. **Risk assessment** – assessment of the impact of risks and prioritization of those risks
8 Components of ERM cut across 4 areas (Continued)

5. Risk response – how management will respond to the risks an institution faces (e.g., mitigate the risk, or share the risk)

6. Control activities – policies and procedures that an institution establishes to ensure that it responds to risks

7. Information and communication – identification and communication of the right information to the right people

8. Monitoring – monitoring and taking corrective action as needed

To be successful, risk must be managed across the 4 areas, the 8 components, and at each organizational level (i.e., functional unit, department, school, and the institution as a whole).
Assessing Institutional Financial Strength

In May 2015, in context of our UAF Power Plant Bond issue, Moody’s affirmed the University’s Aa2 credit rating but revised the outlook from stable to “negative”. S&P credit rating for the University remains AA- and stable.

Notes:
• The State of Alaska has been assigned a “negative” outlook by both rating agencies, Moody’s and S&P.
UA will be Financially Healthy if It...

1. Achieves market leadership as demonstrated by
   • Global reputation
   • Top-ranked programs
2. Increases Enrollment
3. Attracts and retains top students and faculty
4. Enhances diversity of funding sources by having
   • Multiple business lines and revenue sources
   • Low reliance on state support
5. Develops strong donor and community support
6. Maintains access to debt markets at attractive rates by exhibiting
   • Strong balance sheet
   • Prudent debt management
   • Sustainable academic business plan
Board needs to be aware of Areas of Institutional Risks

**Note**: I wish to refer to my *Presentation* on September 19, 2014, titled “Common Issues & Risks for Audit Committee Focus” *(attached).*

1. Cyber security
2. Aging infrastructure and systems
3. Title IX – campus sexual assault
4. Declines in research funding and state support
5. Declining Enrollment
6. Inflating costs such as energy and healthcare
7. Philanthropy and investment returns
8. Managing talent
9. Shifts in competition and consumer demand for higher education
### What is a Risk Map?

A “risk map,” plots probability and impact of risk. It is a good tool for assessing the risks that have been identified and deciding how to respond to them.

<table>
<thead>
<tr>
<th>Impact</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Accept</td>
</tr>
<tr>
<td></td>
<td>Low Risk</td>
</tr>
<tr>
<td>High</td>
<td>Mitigate &amp; Control</td>
</tr>
<tr>
<td></td>
<td>Medium Risk</td>
</tr>
<tr>
<td></td>
<td>High Risk</td>
</tr>
</tbody>
</table>

- **High** and **Medium Risk** should be **Mitigate & Control**.
- **Low Risk** should be **Accept**.
- **High** and **Medium Risk** in the **Probability** category should be **Control**.
In general, there are 4 responses to risk, which also are depicted on the risk map:

- **Accept**
- **Control**
- **Share**
- **Mitigate and Control**

When both the impact and the probability are low (i.e., in the lower left quadrant), institutions would be likely to simply accept the risk.

When both the probability and the impact are high (i.e., in the top right quadrant), institutions would be well advised to design controls that would, in totality, reduce the risk to an acceptable level. In this case, management would design appropriate controls under the oversight of the board.
How is Cyber Risk managed?

1. Measures for protection
   - Real-time data availability
   - Data retention and auditing
   - Identity Management
   - Resilient infrastructure
   - Encryption/VPNs
   - Routing & resource constraints

2. Measures for threat detection
   - Provide data for analysis
   - Threat analysis
   - Blacklists & whitelists
   - Restrict resources
   - State & integrity

3. Measures for remediation
   - Provide awareness of vulnerabilities and remediations
   - Vulnerability notices
   - Patch development
   - Reputation sanctions
   - Investigation & measure initiation

4. Legal Remedies
   - Legal remedies may also institute protective measures
   - Identity Management
   - Resilient infrastructure
   - Encryption/VPNs
   - Routing & resource constraints

- Intergovernmental agreements and cooperation
- Contractual service agreements and federations
- Criminal law
- Indemnification
- Regulatory/administrative law

= information exchange for analysis
= information exchange for actions

Public Interest Report 2012
Goodman-Lukasik-Rutkowski Model
http://fas.org/pubs/pir
What is the Role of the Board?

- Setting the correct tone and demonstrating strong commitment to ERM

Principal benefits of ERM*
- Demonstrates compliance (92%)
- Improves organizational performance & efficiency (69%)
- Reduces cost of risk (54%)

*AON survey on ERM