ERM: Lessons Learned and Tools Used from One University's Nearly 10-Year Implementation Journey

Margaret “Peggy” Zapalac
Director
University Risk and Compliance

Larry Keller
Management Advisor
Objectives

- Overview of ERM
  - Understand the key elements and benefits of an ERM program

- ERM at Texas A&M University
  - Implementation journey
  - Risk assessment process
  - Tools used
  - Challenges looking forward
About Texas A&M University

- Texas’ first public institution of higher learning - opened Oct. 4, 1876 (Land, Sea, and Space-grant federal designations)
- Main campus located in College Station, Texas with over 50,000 students, 2,600 faculty, and 4,800 employees
  - Other locations: Galveston, TX; Qatar; Costa Rica; Italy; Mexico
- Over 850 student-led organizations
- Conduct research valued at over $700 million annually
- Large campus
  - 5,100 + acres
  - 600 + buildings and housing for 10,000 students
  - golf course and an airport
  - 5 utility plants and 2 waste water treatment facilities
- Mergers and outsourcing
  - Health Science Center (July 2013): college of medicine, dentistry, nursing, pharmacy; Law School
  - Outsourcing loss of 1,115 employees
ERM Definition (COSO)

A process, affected by an entity’s board of directors, management, and other personnel,

applied in strategy setting across the enterprise,

designed to identify potential events (risks) that may affect the entity and to manage risk to be within the entity’s risk appetite (tolerance)

to provide reasonable assurance regarding the achievement of the entity’s objectives.
COSO Eight ERM Components

- **Interrelated/integrated with management processes**
  - **Internal environment** (tone, philosophy, executive mgmt. commitment)
  - **Objective setting** (objectives align with mission and are within risk appetite)
  - **Event identification** (risks are identified from internal and external events)
  - **Risk assessment** (likelihood and impact analyzed)
  - **Risk response** (processes in place to manage, mitigating strategies to avoid, accept, reduce, transfer, share)
  - **Control activities** (policies and procedures to ensure risk response are effectively carried out)
  - **Information and communication** (relevant, effective, and timely)
  - **Monitoring** (ongoing management activities and separate evaluations)
NACUBO’s Eight Key Elements

- Includes support from the top and involvement of personnel at all levels
  
  - **Senior management commitment**
  
  - **Risk management owner** (designate chief risk officer responsible to implement the ERM program)
  
  - **ERM framework/process and common language**
  
  - **Communication** (entity’s objectives clearly defined and communicated throughout the organization—risks impact achievement of objectives)
  
  - **Risk management process in place** (ability to assess risks and take timely corrective action to mitigate risks)
  
  - **Monitoring** (Internal Audit involved; include also management, unit heads, Compliance Program personnel, etc.)
  
  - **Human resources processes** (establish accountability)
  
  - **Effective training** (able to mobilize staff)
Benefits of ERM (COSO)

- **Aligning risk appetite and strategy** – Management considers the unit’s risk appetite in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks.

- **Enhancing risk response decisions** – Enterprise risk management provides the standards to identify and select among alternative risk responses – risk avoidance, reduction, sharing, and acceptance.

- **Reducing operational surprises and losses** – Universities gain improved capability to identify potential events and establish responses, reducing surprises and associated costs/losses.

- **Identifying and managing multiple and cross-enterprise risks** – Every enterprise faces a myriad of risks affecting different parts of the organization. Enterprise risk management facilitates effective response to the interrelated impacts, and integrated responses to multiple risks.

- **Seizing opportunities** – By considering a full range of potential events, management is positioned to identify and proactively realize opportunities.

- **Improving deployment of capital** – Using risk information allows management to effectively assess capital needs and enhance capital allocation.
TAMU Realized ERM Benefits

• Value added process
  - Involve participants in identifying and managing risks
    *active as part of the solution*
  - Increase participant’s exposure to other areas
    *enhances knowledge of operations*
  - Increase risk consciousness in decision making
    *provides new perspective*
  - Focus resources and efforts on high risk areas
    *breaks down barriers and demonstrates priorities that are used*
TAMU’s ERM Early Beginning

• In 1999, Management Advisory Services was established
  - to assist management and respond to requests for objective consulting services

• In 2004, University Risk and Compliance was established
  - incorporated management advisory services with two new initiatives
    o Enterprise Risk Management
    o University Compliance
ERM Drivers

- Management (CEOs, Provost, CFOs)
- Board Regents
- Audit Committees
- Auditors (Internal and External)
- Significant Events
Texas A&M University’s ERM Implementation Plan

• Introduce ERM concepts to campus personnel
  – Presentations to units, training/conferences, meetings with unit heads and executive management

• Perform risk assessments
  – University-wide risk assessment
  – Tier I areas reporting to the President and other major functional areas (required)
  – Tier II units reporting to Tier I areas as requested
  – Tier III and beyond provided tools and training for on-going self-assessments as requested
ERM at Texas A&M University

• Top down approach focusing on the University-wide Risk Assessment
    o Participants selected to provide wide university perspective
    o Main actions
      ▪ Identify major risks facing the University
      ▪ Identify the mitigating activities for the top risks, including the accountable responsible person for the mitigating activities
  - Review of significant mitigating activities (2008, 2010 and 2012)
    o Walk-through performed on a sample of mitigating activities
ERM Governance

- System Policy 03.01 (Aug. 2008, updated June 2010)
- President’s Memorandum (Sept. 2009)
- Internal audit report on ERM (Sept. 2010) and follow-up audit (Feb. 2012)
- Standard Administrative Procedure 03.01.01.M0.01 (March 2011)
Common Risk Language

• Risk
  Any event or action that adversely impacts the organization’s ability to achieve its objectives (compliance, strategic, operational, reputational, financial, technology, fraud, etc.)

• Mitigating activities/strategies
  Actions, procedures, and processes used to manage and monitor risks (limit, avoid, accept, transfer, share)

• Risk ranking
  Prioritize and rank (high, medium, low)
  – Impact (consequences)
  – Probability of occurrence (likelihood of happening)

• Risk assessment
  Process used to identify, prioritize, and document risks, mitigating strategies, monitoring processes, and any gaps

• Risk tolerance/appetite (conservative - moderate)
Risks Categories

Risk: Any event or action that adversely impacts the organization’s ability to achieve its objectives

- **Strategic**
affects the University’s ability to achieve goals and objectives, competitive and market risks, etc.

- **Financial**
affects loss of assets—equipment, funds, resources, fraud, etc.

- **Operational**
affects on-going management processes and procedures, fraud, etc.

- **Reputational**
affects reputation or brand, public perception, political issues, etc.

- **Technology**
affects the University’s electronic processes, equipment, and data storage, etc.

- **Compliance**
affects compliance with internal and external laws and regulations, safety and environmental issues, litigation, conflicts of interests, etc.
## Ranking the Risks

**Impact**

*Effect on achieving objectives, the consequences*

<table>
<thead>
<tr>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>show-stopper/loss of program, significant wide spread injuries, death, large loss (%/$ of budget, rev, ex), criminal penalty, liability</td>
<td>inefficient and moderate loss, significant extra/rework, fines, moderate/minor injury</td>
<td>little to no effect, warning, extra work, reprimand, small limited loss</td>
</tr>
</tbody>
</table>

**Probability**

*Likelihood that the risk will happen*

<table>
<thead>
<tr>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>will happen frequently, occurs often, on-going event, predictable, one-time event that may recur</td>
<td>will happen infrequently, sometimes occurs, unpredictable</td>
<td>will seldom happen, infrequent, rarely happens, has not happened</td>
</tr>
</tbody>
</table>
Risk Assessment Steps

- Review mission and strategic plan/goals/objectives
  Identify major activities and functions

- Identify and rank risks
  Prioritize considering impact and probability

- Identify and document mitigating activities
  Evidence of activity occurring and designated accountable person/position

- Review monitoring and executive reporting processes
  Supervisory reviews, managerial oversight, communication flows, and other assurances gained by management that risks are effectively managed

- Follow-up: Assess effectiveness of mitigations
  Perform a limited review/walk through-focusing on significant mitigating activities of highest ranked risks; review mitigations are adequate and working as planned
Facilitated Risk Assessments

• Meeting scheduled by Head of Unit (2-hours)
  - Attendees include direct reports and others
  - May need two meetings
  - Prep work before meeting/homework afterwards

• Two person team - facilitator and scribe

• Equipment
  - Computer and projectors
  - Handouts (list of risks, ranking criteria, prior footprints)
  - Anonymous voting equipment
    o Results posted immediately, can add to or edit risks or re-vote based on discussion, ability to vote or abstain

• Risk footprint and mitigation worksheets provided after meeting
Risk Assessment Tools

- Facilitated sessions
- Excel spreadsheets
  - Color coded, easy to use, linked w/macros
  - Free (developed by David B. Crawford, UTS)
  - Available on URC website: http://universityrisk.tamu.edu/
- Voting software and touch pad equipment
  - Anonymous ranking of impact and probability
- Data management software for entity-wide data
Challenges Looking Forward

- Maintaining momentum
  - Organization and/or leadership changes
- Keeping University-wide and unit risk assessments current and up-to-date
- Providing effective communications regarding University-wide risks and mitigations (e.g., responsible person and oversight)
- Enhancing monitoring (resources to perform walk-throughs for university-wide and unit assessments)
Questions?

Contact Information: Peggy Zapalac
Director, University Risk Management
m-zapalac@tamu.edu
979-845-8115

Larry Keller
Management Advisor
l-keller@tamu.edu
979-862-7739

Websites: http://urc.tamu.edu/
http://universityrisk.tamu.edu/