North Carolina Enterprise Risk Management in Higher Education eSymposium

ERM Tools That Work

Oct. 12, 2011
ERM Definition (COSO)

- A process, effected by an entity’s board or directors, management and other personnel, applied in strategy setting across the enterprise,

  designed to identify potential events that may affect the entity, and manage risk to be within the entity’s risk appetite,

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

COSO’s eight ERM components are interrelated and integrated with management processes

- **Internal environment** (tone, philosophy, executive management 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

- NACUBO’s key elements include support from the top/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)
ERM Drivers

- Management (CEOs, CFOs)
- Boards
- Audit Committees
- Auditors (Internal and External)
- Significant Events
Definition of a Risk

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

**Risks**

- **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.

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

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

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

- Increase risk consciousness in decision making
- Enhance planning and problem solving skills
- Improve allocation of resources
- Focus resources and efforts on key high risk areas
- Enhance capability to identify potential events and establish responses (reducing operational surprises and losses)
- Involve participants as part of the solution and active in identifying and managing risks
- Increase understanding of how mitigating activities/controls affect risks
- Identify and manage cross-enterprise risks
- Provide integrated responses to multiple risks
- Identify events representing opportunity
Risk Assessment Steps

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

- Identify and rank risks
  Consider 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, oversight, communication flow, assurances gained by management that risks are effectively managed

- Follow-up with a walk-through/limited review
  Focus on significant mitigating activities of highest ranked risks; review mitigations are effective and working as planned
Planning a Risk Assessment

- Meet with the head of the unit/area
  - ERM overview/briefing (terminology and process)
  - Ensure unit vision, mission, objectives, and/or strategic plan are current

- Schedule risk assessment meeting(s)
  - Consists of one or more two-hour meetings
  - Can be conducted during a staff meeting or retreat
  - Participants include the unit head, direct reports, and others knowledgeable about operations (size depends on the unit)
  - Facilitated format (one facilitator and one scribe)
  - Participants given overview of ERM
  - Participants identify risks prior to the meeting
    - Strategic, compliance, financial, technology, operational, reputational
  - Flexible – risks are added/edited during meeting
Risk Assessment Tools

- Excel spreadsheets
  - Easy to use, color coded risks, linked with macros
  - Template available at no cost
    - Developed by David B. Crawford, Univ. of Texas System

- Voting software and touch pad equipment
  - Used to rank impact and probability
  - Anonymous results
  - Results shown immediately
  - Ability of participants to vote or abstain
  - Ability to revote after discussion and comments
## Ranking the Risks

<table>
<thead>
<tr>
<th>Impact</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High</strong></td>
<td><strong>High</strong></td>
</tr>
<tr>
<td>show-stopper, significant injuries or death, large loss (i.e., &gt;50% of budget), criminal penalty, loss of program, liability</td>
<td>will happen frequently, occurs often, on-going event, predictable, one-time event that may recur</td>
</tr>
<tr>
<td><strong>Medium</strong></td>
<td><strong>Medium</strong></td>
</tr>
<tr>
<td>inefficient and moderate loss, significant extra work/rework, fines, reputational effects, moderate/minor injuries</td>
<td>will happen infrequently, sometimes occurs, unpredictable</td>
</tr>
<tr>
<td><strong>Low</strong></td>
<td><strong>Low</strong></td>
</tr>
<tr>
<td>little to no effect, warning, extra work, reprimand, limited loss</td>
<td>will seldom happen, infrequent, rarely happens, has not happened</td>
</tr>
<tr>
<td>Research Development, Programs and Facilitation</td>
<td>IMPACT</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>Decrease in State support</td>
<td>h</td>
</tr>
<tr>
<td>Lack of research management information</td>
<td>h</td>
</tr>
<tr>
<td>Ineffective metrics for evaluating programs and personnel</td>
<td>h</td>
</tr>
<tr>
<td>Lack of seed/incentive funding</td>
<td>h</td>
</tr>
<tr>
<td>Lack of industrial funding/partnerships</td>
<td>m</td>
</tr>
<tr>
<td>Research Finance and Administration</td>
<td></td>
</tr>
<tr>
<td>Noncompliance with policies, rules, and laws</td>
<td>h</td>
</tr>
<tr>
<td>Untimely reporting</td>
<td>h</td>
</tr>
<tr>
<td>Not rewarding academic excellence</td>
<td>h</td>
</tr>
<tr>
<td>Lack of coordinated research administration</td>
<td>h</td>
</tr>
<tr>
<td>Unfunded mandates</td>
<td>h</td>
</tr>
<tr>
<td>Not following protocols</td>
<td>h</td>
</tr>
</tbody>
</table>
Impact: Lack of coordinated research management

1. High
   - 67%

2. Medium
   - 22%

3. Low
   - 11%
Probability:
Lack of coordinated research management

1. High
   - 11%

2. Medium
   - 56%

3. Low
   - 33%
## Risk Footprint Example

<table>
<thead>
<tr>
<th>ACTIVITIES</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Research Finance &amp; Administration</td>
<td>HH</td>
<td>HH</td>
<td>HH</td>
<td>HM</td>
<td>HM</td>
<td>HL</td>
</tr>
<tr>
<td>Noncompliance with policies, rules, laws</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Untimely reporting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not rewarding academic excellence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lack of coordinated research admin.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unfunded mandates</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not following protocols</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Research Development, Programs &amp; Facilitation</td>
<td>HH</td>
<td>HM</td>
<td>HM</td>
<td>HM</td>
<td>MH</td>
<td></td>
</tr>
<tr>
<td>Decrease in State support</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lack of research management information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ineffective metrics for evaluating programs and personnel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lack of seed/incentive funding</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lack of industrial funding/partnerships</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Risks ranked considering both their impact and probability:

**Impact** - the consequence(s) of the risk occurring (H=High, M=Medium, L=Low)

**Probability** - the likelihood of the risk occurring (H=High, M=Medium, L=Low)

- **HH** = HH, HM
- **HL** = HL, MH
- **MM** = MM, ML, LH
- **LM** = LM, LL
Mitigating Activities

- Excel spreadsheet(s) used to capture what is in place to manage/mitigate the risks
  - Organized by tabs for each major activity/category
  - Includes:
    - Description of the activity
    - Who (what position) is accountable/responsible for performing the activity
    - Evidence/documentation of the activity
    - Monitoring or supervisory controls over the activity
    - Communication/executive management reporting
## Mitigating Activities Example

<table>
<thead>
<tr>
<th>Risks</th>
<th>Research Finance &amp; Administration</th>
<th>Evidence of Control Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Noncompliance with policies, rules, laws</td>
<td>x</td>
<td>Grant training for proposal development group, Research Foundation personnel, and dept staff. New faculty orientation. Online training.</td>
</tr>
<tr>
<td>Untimely reporting</td>
<td>x</td>
<td>Presentation to legislature (Govt. Affairs/VPR/President), Publications/Website. Research road show - committee.</td>
</tr>
<tr>
<td>Not rewarding academic excellence</td>
<td>x</td>
<td>Cost sharing, review procedures, signed approval documents.</td>
</tr>
<tr>
<td>Lack of a coordinated research admin. structure</td>
<td>x</td>
<td>Signature sheets. Email notification for changes.</td>
</tr>
<tr>
<td>Unfunded mandates</td>
<td>x</td>
<td>Online training. Forms signed.</td>
</tr>
<tr>
<td>Not following protocol</td>
<td></td>
<td>Manager oversight and verbal communication with Sr. mgmt</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mitigating Activities Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training</td>
</tr>
<tr>
<td>x</td>
</tr>
<tr>
<td>Marketing &amp; communication to Legislators &amp; Public</td>
</tr>
<tr>
<td>x</td>
</tr>
<tr>
<td>Policies/Forms</td>
</tr>
<tr>
<td>x</td>
</tr>
<tr>
<td>Signature authority - based on delegation</td>
</tr>
<tr>
<td>x</td>
</tr>
<tr>
<td>PI certifications</td>
</tr>
<tr>
<td>x</td>
</tr>
<tr>
<td>Office of research compliance</td>
</tr>
<tr>
<td>x</td>
</tr>
<tr>
<td>Budgetary control</td>
</tr>
<tr>
<td>x</td>
</tr>
</tbody>
</table>

### Risks

- Noncompliance with policies, rules, laws
- Untimely reporting
- Not rewarding academic excellence
- Lack of a coordinated research admin. structure
- Unfunded mandates
- Not following protocol
Communications with executive management
  ◦ Meetings and correspondence while getting ERM off the ground and continually adjusting to changes in executive management (maintaining champions/President Memo)

Reporting up/down/cross
  ◦ Entity-wide risk assessment (footprint, mitigations)
  ◦ Walk-through report
  ◦ Internal audit report
  ◦ Unit level assessments reported up to next level
  ◦ University policy/rules (TAMU’s SAP 03.01.01.M0.01)

Data management and recordkeeping
  ◦ Electronic records and retention
    • ERM enterprise software, Individual unit Excel spreadsheets
Enterprise Risk Management

A management tool that enhances ability to achieve objectives by effectively identifying, planning for, and responding to risks.

Understanding Risks … Managing Operations … Reaching Goals

Contact Information
Margaret (Peggy) Zapalac
m-zapalac@tamu.edu
University Risk and Compliance
Texas A&M University
http://universityrisk.tamu.edu
Questions?