Enterprise Risk Management

Assessing and Managing Risks at Texas A&M University

IIA Brazos Valley Chapter
July 17, 2014
Objectives/Outline

• Overview of ERM
  – Key elements and benefits

• ERM at Texas A&M University
  – ERM and Compliance structure

• Risk Assessments
  – Strategies/tools
  – BV IIA Chapter
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
  – Health Science Center
  – Other locations: Galveston, TX; Qatar; Costa Rica; Italy; Mexico
• Over 58,000 students, 2,750 faculty, and 5,500 employees;
• 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
  – 4 utility plants and 2 waste water treatment facilities
• Mergers, acquisitions, and outsourcing
  – Health Science Center (July 2013): College of Medicine, Dentistry, Nursing, Pharmacy
  – Law School
  – Outsourcing loss of 1,115 employees (Landscaping, Maintenance, Dining Services, Custodial)
• Part of a large System (11 Universities and the HSC, 7 agencies, 2 service units)
University Risk and Compliance

- **URC (established 2004)**
  - Enterprise Risk Management
  - University Compliance
  - Compliance Officer (2012)
    - Title IX Coordinator, ADA Coordinator, Clery Committee Chair, etc.
  - Management Advisory Services
  - Rules and Standard Administrative Procedures
  - Audit Liaison
  - Other
    - EthicsPoint University Contact (2014)
    - Code Maroon
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.
ERM and Compliance Drivers

- Management (CEOs, Provost, CFOs)
- Board of Regents
- Audit Committees
- Auditors (Internal and External)
- Significant Events
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.
ERM Benefits at TAMU

• 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*
ERM and Compliance Governance

• ERM
  - 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)

• Compliance
  - U.S. Federal Sentencing Guidelines
  - System Policy 16.01 (May 2012, updated Jan. 2014)
  - System Regulation 16.01.01 (May 2012)
ERM at Texas A&M University

• Implemented ERM using a top down approach
  – Focus on University-wide risks, then major units
  – TAMU risk assessment performed in 2004
    • Facilitated session (facilitator/scribe): participants selected to provide wide university perspective
    • Main action: identify major risks facing the University and mitigating activities
    • Evidence of activity
    • Monitoring/supervisory actions
    • Communication/reporting to management
    • Written report includes “Opportunities for Improvement”
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)**
Risk Types

**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.
- **Operational** affects on-going management processes and procedures, fraud, etc.
- **Financial** affects loss of assets-equipment, funds, resources, 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

(1) **High**
show-stopper/loss of program, significant wide spread injuries, death, large loss (%/$ of budget, rev, ex), criminal penalty, liability

(2) **Medium**
inefficient and moderate loss, significant extra/rework, fines, moderate/minor injury

(3) **Low**
little to no effect, warning, extra work, reprimand, small limited loss

Probability
Likelihood that the risk will happen

(1) **High**
will happen frequently, occurs often, on-going event, predictable, one-time event that may recur

(2) **Medium**
will happen infrequently, sometimes occurs, unpredictable

(3) **Low**
will seldom happen, infrequent, rarely happens, has not happened
Risk Assessment Steps

• Review mission and strategic plan, goals, and/or 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
## 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/](http://universityrisk.tamu.edu/)
- **Voting software and touch pad equipment**
  - Anonymous ranking of impact and probability

### Risk Matrix

<table>
<thead>
<tr>
<th>RISKS</th>
<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</td>
<td>Finance &amp; Administration</td>
<td>Noncompliance with policies, rules, laws</td>
<td>Untimely reporting</td>
<td>Increasing in cost support</td>
<td>Lack of research management structure</td>
<td>Lack of coordinated research efforts</td>
<td>Untimely expenditures</td>
</tr>
<tr>
<td>Research Development, Programs, &amp; Facilitation</td>
<td>Lack of a coordinated research administration</td>
<td>Lack of research management structure</td>
<td>Ineffective metrics for evaluating programs and personnel</td>
<td>Lack of research management structure</td>
<td>Lack of research management structure</td>
<td>Lack of industrial funding/ partnerships</td>
<td></td>
</tr>
</tbody>
</table>

### Evidence of Control Activity

<table>
<thead>
<tr>
<th>Research Finance &amp; Administration</th>
<th>Noncompliance with policies, rules, laws</th>
<th>Untimely reporting</th>
<th>Increasing in cost support</th>
<th>Lack of research management structure</th>
<th>Lack of coordinated research efforts</th>
<th>Untimely expenditures</th>
<th>Not following protocols</th>
<th>Evidence of Control Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Marketing &amp; communication</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Research forms</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Office of research compliance</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Budgetary control</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

### 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, HM
- HL, MH
- MM, ML, LH
- LM, LL
Risk Assessment Exercise

- IIA BV Chapter’s Purpose:

Our mission is to offer a great opportunity for internal audit professionals to network, share learning experiences, and earn CPEs by attending low cost, local training events in the Brazos Valley. We hope to serve members at both large and small organizations, and to promote professional development as a benefit for all in the Brazos Valley.
IIA BV Chapter
Potential Risks

• Not able to attract and retain talented chapter officers
• Chapter not in compliance with IIA rules/requirements
• Inadequate funds/budget for chapter activities
• Lack of awareness of the Chapter (ineffective marketing/communications)
• Inadequate opportunities for professional networking and sharing expertise
• Not offering valued/cost effective CPE
After the Risk Assessment

• Identify mitigating activities
  – What is in place or planned to manage/mitigate
  – Who is doing it
  – How is it documented
  – Who monitors it
  – How are results/status communicated

• Review effectiveness of mitigating activity
  – Is it working as planned
  – Do we need to change anything
Comments/Questions?

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

- Contacts:
  - Peggy Zapalac
    - m-zapalac@tamu.edu
    - 979-845-8115
  - Larry Keller
    - l-keller@tamu.edu
    - 979-862-7739