Enterprise Risk Management

One University’s Approach

Assessing and Managing Risks at Texas A&M University

March 4, 2014
Objectives/Outline

• Overview of ERM
  – Key elements and benefits

• ERM at Texas A&M University
  – ERM and Compliance structure
  – ERM 10 year implementation journey
  – Strategies/tools to prioritize risks and evaluate mitigating activities
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)
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
    - University Compliance
    - Enterprise Risk Management
TAMU’s University Risk and Compliance Office

- University Compliance Officer
  - Coordinator for Title IX, ADA, and Web Accessibility
- Compliance Program
- Rules and SAPs
- Enterprise Risk Management Program
- Risk, Fraud & Misconduct Hotline
- Audit Liaison
- Management Advisory Services
- Code Maroon (Emergency Notification System)
URC Organizational Chart

TAMU President

Vice President for Finance and Administration

Associate Vice President and TAMU Compliance Officer

Compliance Committee (Chair)

Task Force for Campus Emergencies (Co-chair)

Other University-Wide Committees

Enterprise Risk Management
Margaret Zapalac, Director

University Compliance
Annette Wallis, Director

ERM
Management Advisor

MAS
Management Advisor

Audit Liaison
Management Advisor

Compliance Projects
Management Advisor

Compliance Projects
Management Advisor

Rules/SAPs
Management Advisor

Compliance Officer has direct/regular access to the CEO (System Regulation 16.01.01 System Ethics and Compliance)

ADA Compliance (ADA Coordinator and Chair)

Title IX Compliance (Title IX Coordinator and Chair)

Web Accessibility (Web Accessibility Coordinator and Chair)

Clery Committee (Chair)

Drug Free Schools and Communities Act (Chair)

Rules Team (Chair)
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 (CEO, Provost, CFO)
• Board 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 \textit{active as part of the solution}
  – Increase participant’s exposure to other areas \textit{enhances knowledge of operations}
  – Increase risk consciousness in decision making \textit{provides new perspective}
  – Focus resources and efforts on high risk areas \textit{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
  - Focused on University-wide risks
  - Performed first risk assessment in 2004
    - Participants selected to provide wide university perspective
  - 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
  - Reviewed significant mitigating activities (2008, 2010 and 2012)
University-wide Risk Assessment Walk-through

  - Performed by URC personnel
  - Sample of mitigating activities (red risks)
  - Walk-through/review process
    - Inquiries, review documentation, observe procedures
  - Focus on
    - Evidence of activity
    - Monitoring/supervisory actions
    - Communication/reporting to management
  - Written report includes “Opportunities for Improvement”
ERM Risk Assessments

- Perform risk assessments in other units
  - VPs, direct reports to the President, Colleges, major departments or functions, etc.
  - Use facilitated group meetings (facilitator/scribe)
    - 2-hr meeting held with Unit Head and direct reports
    - Identify/rank major risks facing the unit based on mission/goals/objectives (some pre-meeting work done)
    - Identify the mitigating activities for the top risks (mostly done post-meeting)
      - Accountable person responsible for the mitigating activities; documentation/evidence
      - Monitoring/supervisory and reporting activities
    - Management reviews mitigations for effectiveness
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: Any event or action that adversely impacts the organization’s ability to achieve its objectives

**Risk Types**

- **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.
- **Reputational**: affects reputation or brand, public perception, political issues, etc.
- **Technology**: affects the University’s electronic processes, equipment, and data storage, etc.
- **Financial**: affects loss of assets—equipment, funds, resources, fraud, 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

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

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

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

Probability
Likelihood that the risk will happen

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

**Medium**
will happen infrequently, sometimes occurs, unpredictable

**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/
- Voting software and touch pad equipment
  - Anonymous ranking of impact and probability
Risk Ranking Exercise

- Not able to attract and retain talented faculty
- Noncompliance with federal and state laws (Clery Act, ADA, Title IX, etc.)
- Not having a strong commitment to sustainability
- Not having a safe environment for minors on campus (camps, enrichment programs, etc.)
- Incompatible duties/not segregating cash handling duties
Challenges Looking Forward

- Maintaining momentum
  - Organization and leadership changes
- Keeping risk assessments up-to-date
- Coordinating with compliance function
  - Risk assessment, stakeholder groups, etc.
- Providing effective communications regarding University-wide risks and mitigations
  - Responsible persons, walk-through report, compliance plan
- Enhancing monitoring (need resources)
  - Risk assessment walk-throughs
  - Performing compliance reviews, for example
    - Research Certifications (requested by Research)
    - Title IX Self-Assessment
    - Clery Act Reviews
    - Higher Ed Opportunity Act (requested by SFA)
    - Natural Gas Line Incidents (requested by the System Compliance Officer)
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