Enterprise Risk Management, Compliance, and Management Advisory Services: An Integrated Approach

SCCE's Higher Education Compliance Conference

June 13, 2011

Objectives

- Implementing Enterprise Risk Management (ERM) in a decentralized environment
  - Benefits and challenges from a Texas A&M University perspective
- Assessing our risks
  - How Texas A&M University performs risk assessments
- Providing management advisory/consulting services
  - How Texas A&M University uses these services to support ERM and compliance activities

About Texas A&M University

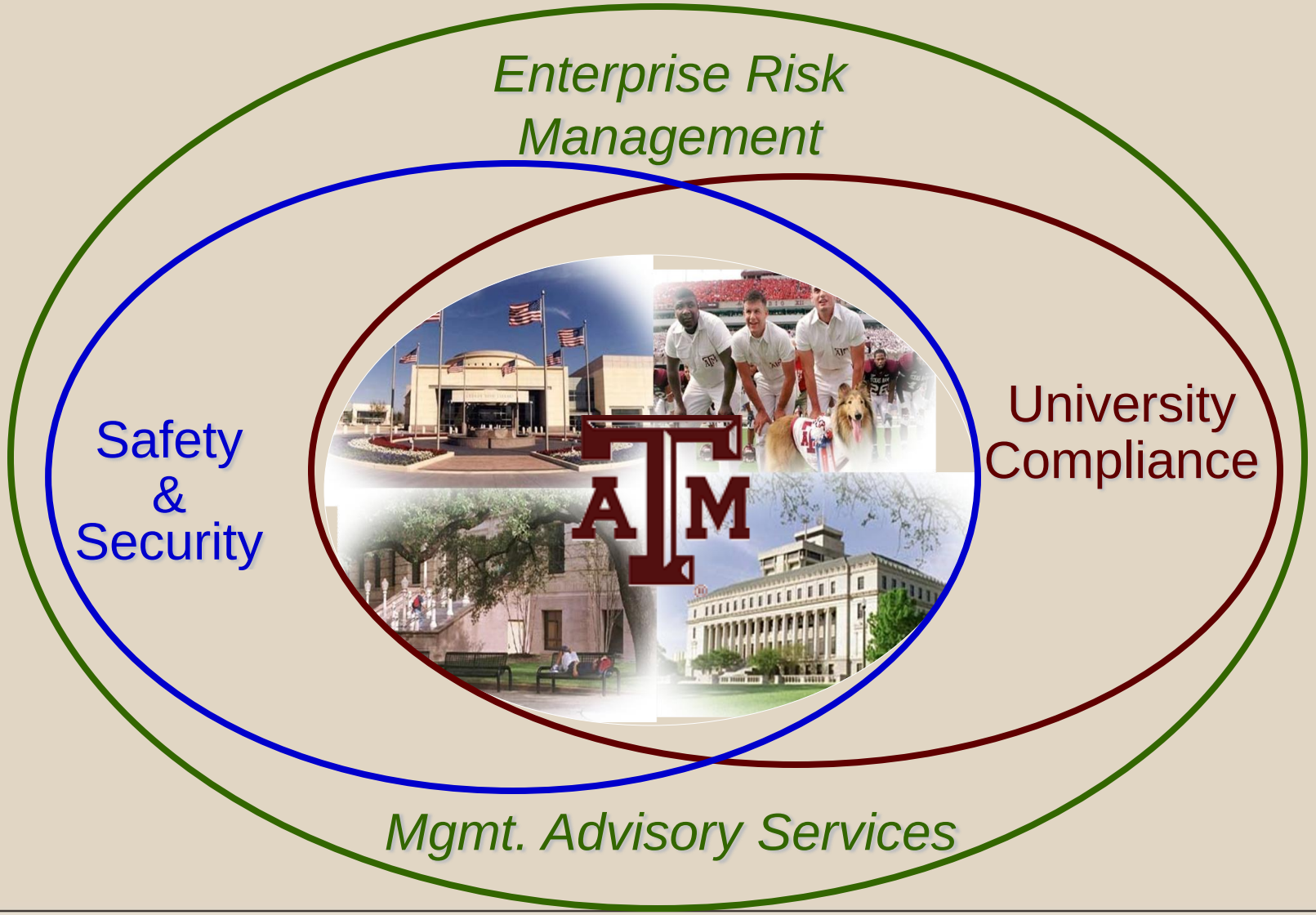
- Texas' first public institution of higher learning - opened Oct. 4, 1876 (Land, Sea, and Space-grant federal designations)
- Located in College Station, Texas with branch campuses in Galveston and Qatar, international centers in Mexico, Costa Rica, and Italy
- Over 49,000 enrolled which includes approx. 2,000 in the Corps of Cadets and 9,000 graduate students
- Large campus - over 5,100 acres with housing for 10,000 students, golf course and an airport
- Conduct research valued at over $630 million annually
- NCAA Division I-A level, 20 varsity sports
- Over 800 student organizations
- More than $492 million available in financial aid (79% of students)
- A member of the Texas A&M University System (11 Univ., 7 agencies, 1 HSC)

Integrated Approach

- 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 that incorporated management advisory services with two new initiatives and a reorganization of Safety and Security (including Environmental Health and Safety and University Police) under one Associate Vice President.
  - Enterprise Risk Management
  - University Compliance

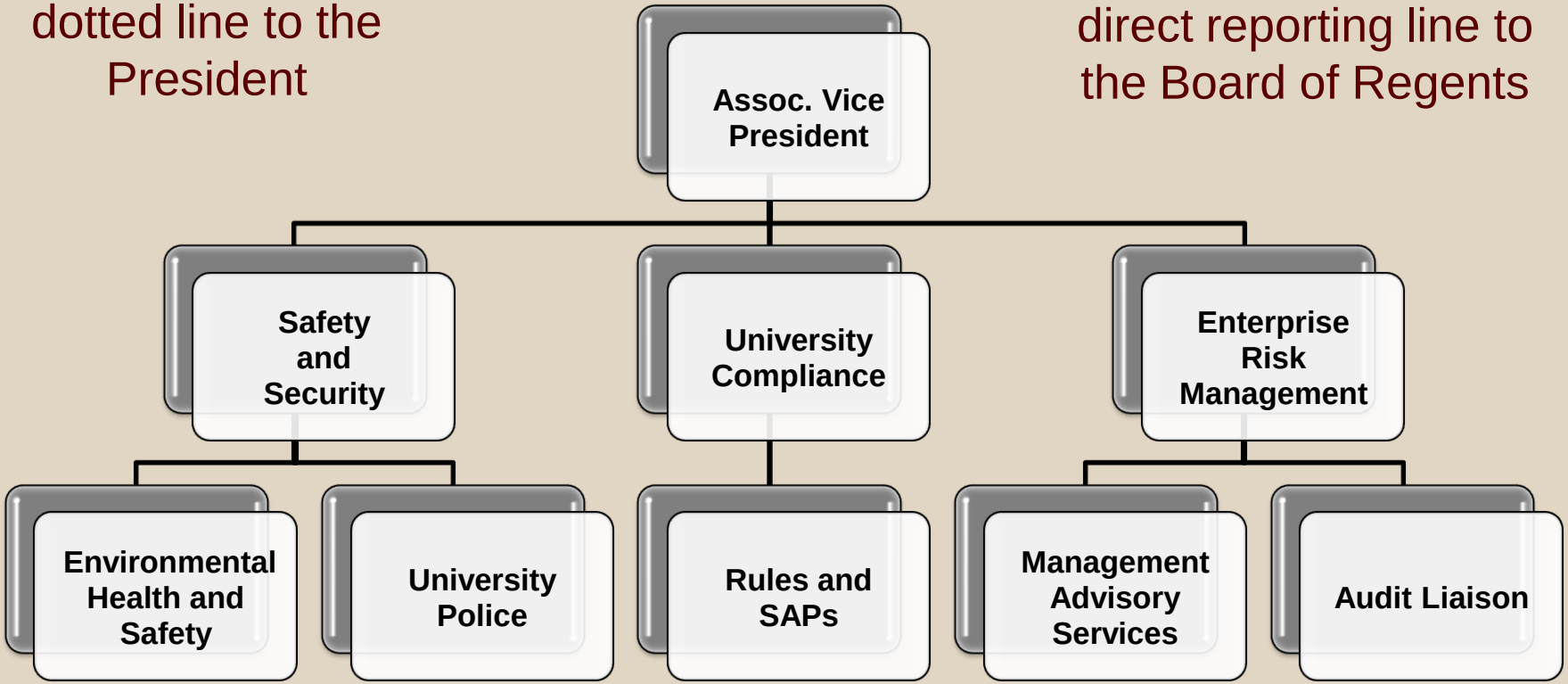
University Risk and Compliance (URC)



URC Organizational Structure

URC has direct reporting line to Vice President for Administration and dotted line to the President

URC coordinates with Internal Audit who is positioned at the System level with direct reporting line to the Board of Regents



Enterprise Risk Management

Definition:

A process applied ***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) in order to provide reasonable assurance regarding the ***achievement of the entity's objectives***.

Drivers:

Events, Management, Audit Committee of the Board of Regents, System Internal Audit

Eight Key Elements of ERM

- Key elements begin with support from the top and involvement of personnel at all levels (NACUBO)
  - Senior management commitment
  - Designated risk officer
  - ERM framework and common language used
  - Risk management process in place to assess risks and mitigating strategies
  - Monitoring (performed at all levels such as managers, Internal Audit, etc.)
  - Human resources processes establish accountability (i.e., included in performance evaluations)
  - Communication (reporting to exec. mgmt., web sites, etc.)
  - University-wide training (required training, policies and procedures, presentations, etc.)

Components of ERM (COSO)

- *Internal Environment (tone, philosophy, risk appetite)*
- *Objective Setting (strategies/goals)*
- *Event Identification (internal/external)*
- *Risk Assessment (ranking/prioritizing)*
- *Risk Response (avoid, reduce, transfer)*
- *Control Activities (policies/procedures)*
- *Information and Communication*
- *Monitoring*

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

ERM at TAMU

- Top down approach
  - First university-wide risk assessment performed in 2004, updated 2006, 2009, and again in 2011.
    - Walk through review of significant mitigating activities (2008 and 2010)
  - Performed risk assessments on major University units (divisions, colleges, auxiliaries, etc.)
- System Policy 03.01 (Aug. 2008, updated June 2010)
- President's Memorandum (Sept. 2009)
- Internal audit report on ERM (June 2010)
- 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)

  - Consider potential impact (consequences)
  - Consider probability of occurrence (likelihood of happening)

- Risk assessment

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

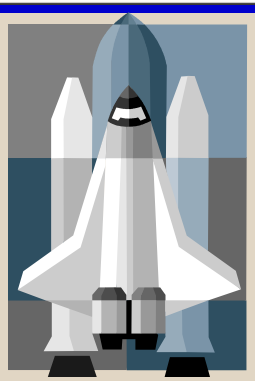
- Risk tolerance/appetite (conservative - moderate)

ERM Risk Categories

Ranking the Risks

Impact

Effect on achieving objectives, the consequences



High

show-stopper, loss of program, wide spread illness/injury, death, large loss (%/$ of budget, revenues, expenses), criminal penalty, liability

Medium

inefficient and extra or re-work, fines, minor injury, moderate loss

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 recurs

Medium

happens infrequently, sometimes occurs, unpredictable

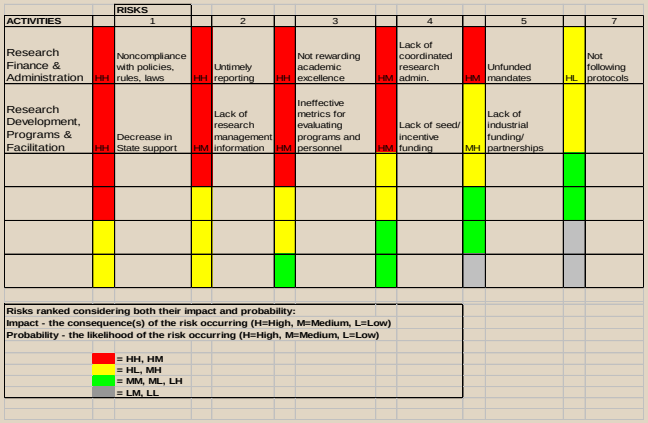
Low

will seldom happen, infrequent, rarely happens, has not happened

Risk Assessment Tools

- Facilitated sessions by URC personnel
- 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/



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

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, HM
= HL, MH
= MM, ML, LH
= LM, LL

- Voting software and touch pad equipment
  - Anonymous ranking of impact and probability
- Data management software to record and report University-wide data

Risk Assessment Steps

Review mission and strategic plan/goals/objectives

Identify major activities and functions

Identify and rank risks

Prioritize by 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, oversight, communication flow, and other 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

Enterprise Risk Management

- **Challenges Looking Forward**
  - Having units perform initial assessment
  - Keeping University-wide and unit risk assessments current
  - Providing effective communications of the University-wide risks and mitigations (e.g., responsible person/position)
  - Enhancing monitoring (resources to perform/assist units with walk-throughs)

Compliance

- Several “red risks” on the university-wide risk assessment
- Specific compliance responsibilities are distributed across the University
  - i.e., Research Compliance; Athletic Compliance; Student Financial Aid; Student Affairs, etc.
  - Individual risk assessments performed for specific compliance areas
- Compliance risks considered as a component of every unit’s risk assessment

University Compliance

- Perform reviews
  - Evaluate if audit issues/recommendations have been effectively addressed (prior to internal audit follow-ups)
  - Evaluate compliance of internal processes with applicable laws, policies, regulations, etc. (i.e., research assurances, web accessibility, HIPAA, etc.)
- Coordinate regulatory reporting
  - Annual Security Report (Clery Act), Annual Fire Report (HEOA)
  - Drug Free Schools and Community Act Biennial Review
- Provide oversight and collaboration
  - ADA Coordinator (Chair, ADA Compliance Committee)
  - Compliance Reporting Committee (Chair)
  - Coordinate with other offices (i.e., General Counsel, System Internal Audit, Equal Opportunity & Diversity)

University Compliance

- Maintain University Rules and Standard Administrative Procedures (SAPs)
  - Coordinate development, review, and approval for new and revised University Rules and SAPs (main and branch campuses)
  - Communicate approved new and revised Rules and SAPs to the University community
  - Coordinate University comments for new and revised draft System Policies and Regulations and interface with the System Policy Office
  - Maintain a central repository with online access to current Rules/SAPs (3-year review period)

- Respond to inquires and provide training regarding University Rules/SAPs and other compliance issues

Management Advisory Services (MAS)

- Established to provide the University community “free” consulting services by experienced staff that understands the environment, operations, policies and rules.
- MAS works in an advisory role with all levels of personnel to address risks and compliance issues, advance the University’s mission and goals, and develop solutions to challenges.
  - Collaboratively work together with management and staff
  - Develop new ideas and action plans that augment/complement the existing structure, processes, and procedures.
  - Integrate effectiveness and efficiency in control procedures
  - Provide training and support

Types of MAS Projects

- Performing walk through reviews following a risk assessment focusing on significant risks and verify mitigating procedures are working as planned
  - Review the responsible person/position, documentation/evidence maintained, monitoring processes, reporting and assurances provided to executive management
- Reviewing the internal control structure for cashiering functions displaced by building renovations or for new revenue streams
- Reviewing draft policies and procedures being updated to address identified risks and internal control weaknesses
- Reviewing the process and assess the time and effort for determining whether to transfer duties to a central processing department
- Reviewing the organizational structure for divisions, colleges, and departments
- Making presentations on emerging compliance issues, risk management, internal controls, fraud, etc.

Types of Reports

- Flexible
  - Formal reports with opportunities/recommendations and management's response and/or action plans
  - One-page summary reports
  - E-mail correspondence
  - Verbal consultations

Audit Liaison

- Established to support management in responding effectively to audits
  - Serve as a point of contact regarding the overall audit process
  - Provide consultative advice and assistance on the audit process
    - Attend audit meetings
    - Review draft audit reports and management responses
    - Advise on options/alternative strategies to address the risks and potential impact of recommendations
  - Provide up-to-date information for executive management
    - Prepare briefing materials used to assist executive management in responding to audit committee inquiries (i.e., audit reports, implementation status of recommendations, etc.)

Questions?

Contact Information:

Margaret “Peggy” Zapalac

Director, University Risk Management

m-zapalac@tamu.edu

979-845-8115

http://urc.tamu.edu