

5th Conference for Effective Compliance Systems in Higher Education

***A Texas A&M University
approach to Enterprise
Risk Management***

June 4, 2007

**Peggy Zapalac, Director of University Risk Management
University Risk and Compliance
<http://universityrisk.tamu.edu>**

Enterprise Risk Management

Definition of ERM:

A process applied across the enterprise,

designed to

identify potential events that may affect the entity
and

manage risk to be within the entity's risk appetite,

that provides

reasonable assurance regarding the
achievement of the entity's objectives.

About Texas A&M University

- Texas' 1st public institution of higher learning, opened Oct. 4, 1876 (Land, Sea, and Space-grant federal designations)
- Located in College Station, branch campuses in Galveston and Qatar, centers in Mexico City and Italy
- Fall 06 enrollment of 45,380, including approx. 1,800 in the corps of cadets
- Large campus (5,200 acres including a 434 acre research park) with 10,000+ in student housing opportunities
- Conduct research valued at over \$500 million annually
- NCAA Division I-A level in 20 varsity sports
- Over 700 student clubs and organizations
- More than \$350 million available in financial aid

Enterprise Risk Management

- Texas A&M University (TAMU) management supports ERM and compliance activities and the university-wide efforts to identify and manage risks and compliance requirements
- TAMU established the University Risk and Compliance Office (Apr. 04) as part of a university reorganization
 - New responsibilities included
 - Implementing ERM
 - Implementing a University Compliance Program
 - Establishing Safety and Security Office
 - Providing management advisory services

University Risk and Compliance-TAMU

*Enterprise Risk
Management*

**Safety
&
Security**

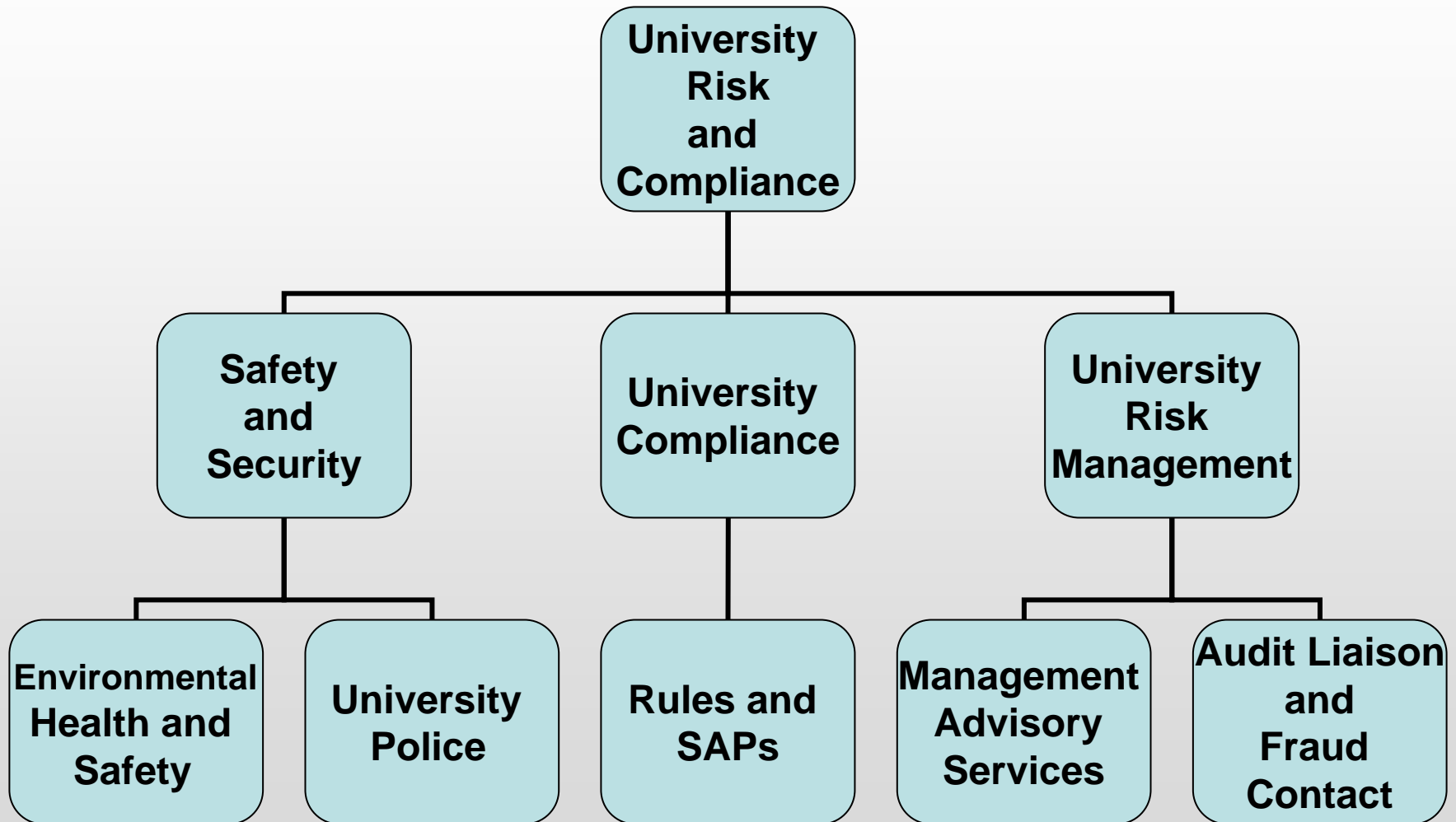
**Compliance
&
Rules**



Advisory Services

URC Organizational Structure

URC centrally positioned with reporting line to Provost and President



Enterprise Risk Management

Eight Key Elements (NACUBO)

- Key elements begin with support from the top and involvement of personnel at all levels
 - Senior management commitment
 - Designated risk officer – established a University Risk and Compliance office (URC)
 - ERM framework and common language used
 - Risk management process in place to assess risks and mitigating strategies
 - Monitoring performed by managers, the University Compliance Program, and internal audit
 - Human resources processes establish accountability
 - Communication via web sites, presentations, etc.
 - University-wide training (ethics, information security, etc.)

Five broadly categorized maturity levels

TAMU's ERM

Implementation Plan

- Introduce ERM concepts to TAMU
- Perform risk assessments
 - University-wide
 - Tier I – areas reporting to the President and other major functional areas
 - Tier II – units reporting to Tier I areas
 - Tier III and beyond-provide tools and training for on-going self-assessments
- Executive Management Reporting and Monitoring
 - Status reviews-compliance
- Continuous, on-going process

Enterprise Risk Management at TAMU - Risk Assessments

- Risk Management Discussion Group
 - Compliance committee
- Provost
 - URC, Environmental Health Safety, and Police
 - Colleges-financial
 - Assessment
 - International Programs
- Research
 - Research Compliance
- Student Affairs
- Athletics
- Athletic Compliance
- Information Technology
- Facilities
- Finance (Controller)
 - Transportation Services
 - Accounts Payable
 - Council of Sr. Business Administrators
- Communications and Marketing
- Governmental Affairs
- Diversity
- Development
- TAMU – Galveston
- TAMU – Qatar
- Academics
 - College of Science

Enterprise Risk Management at TAMU

University-wide Risk Management Discussion Group (Fall 2004 and updated in Fall 2006)

- Members were selected to provide a University-wide perspective
- Actions
 - Identified major risks facing the University
 - Identified mitigating activities for the top risks and the accountable/responsible person for the mitigating activities

Examples of Major University Risks

- Risk of non-compliance w/State, Federal requirements (FERPA, HIPAA, copyrights, intellectual properties, student financial aid, international laws on immigration, etc.)
- Risks associated with large scale open events (i.e., conferences, camps, visitors, student groups, the corps of cadets, and athletic events) - open environment.
- Safety and security risks – culture (reporting, training, corrective actions), instructional environments (classrooms, teaching and research labs, University vessels, fieldwork, equipment use, etc.), student activities, travel to University sponsored events, etc.

Examples of Major University Risks

cont'd

- Reduced funding (federal, state, and/or local) combined with an anticipated growth factor
- Risks of implementing large scale IT improvements (student information, financial, IT infrastructure, etc.)
- Risk of potential IT failures (loss of systems, loss of data, theft of data, intrusions/malware, obsolescence, unapproved release of confidential/sensitive data, etc.)
- Noncompliance in research activities (conflicts of interest, research misconduct, etc.)
- Deteriorating facilities and infrastructure (campus buildings, student housing, physical plant operations, funding repairs/maintenance, etc.)

Enterprise Risk Management

Safety and security risks - changing the safety culture

- **TAMU Initiatives**

- **Expanding the mission and role of Environmental, Health, and Safety**
- **Implementing the Safety Hotline (979)862-SAFE or <http://safetyhotline.tamu.edu/>**
- **Including safety issues in President's Council meetings**
- **Enhancing the Safety Program**

Enterprise Risk Management

Risk of noncompliance in research activities

- **TAMU initiatives**
 - **Enhancing the Office of Research Compliance**
 - **Performing Compliance Program projects**
 - **Implementing screening export control software**
 - **Obtaining accreditation for Institutional Review Board**
 - **Broadening Principal Investigator participation on the Patriot Act Task Force**

Performing a Risk Assessment

- Two person team -determine who will be the facilitator and who will scribe
- Arrange with division/dept. head
- Typically consists of three 2-hour meetings several days apart
- Attendees include division/dept head, direct reports, and others
- Ideal group size depends on unit
- Prep before the meeting(s)

Risk Assessment Steps

Review mission/strategic plan/goals/objectives

Identify activities

Identify and rank risks

Identify mitigating activities

Review monitoring processes

Common Risk Language

– Risk

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

– Risk assessment

- The process used to identify and document risks, mitigating strategies, monitoring processes, and any gaps

– Risk ranking

- Prioritized and rank (high, medium, low)
 - Consider potential impact (consequences)
 - Consider probability of occurrence (likelihood of happening)

– Mitigating activities/strategies

- Actions, procedures, controls, and processes used to manage and monitor risks (limit, avoid, accept, transfer, share)

Categories of Risk

Strategic

(affects the University's ability to achieve goals and objectives, and competitive and market risks, etc.)

Reputational

(affects reputation, public perception, political issues, etc.)

Risks



Compliance

(affects compliance with laws and regulations, safety and environmental issues, litigation, conflicts of interests, etc.)

Financial

(affects, fraud, loss of assets, technology risks, etc.)

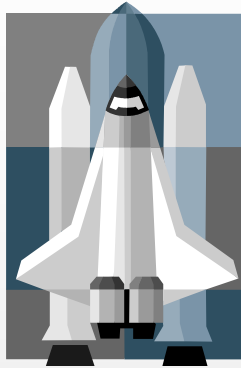
Operational

(affects on-going management processes and procedures, etc.)

Ranking the Risks

Impact

Effect on achieving objectives, the consequences



High

show-stopper, significant injury or death, large loss (>50% of budget), criminal penalty, loss of program, liability

Medium

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

Low

little to no effect, warning, extra work, reprimand, 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

will happen infrequently, sometimes occurs, unpredictable

Low

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

Risk Assessment Tools

- Excel spreadsheets
 - Linked with macros
 - No cost (developed by David B. Crawford, UTS)
- Optionpower voting software and touch pad equipment
 - Anonymous ranking of impact and probability
 - Ability to vote or abstain

Risk Assessment Tools

Excel Worksheets - Activities



Set Up Activity Sheets

PRIORITIZED CONSOLIDATED ACTIVITIES

- 1 Research Development, Programs, and Facilitation
- 2 Research Finance and Administration
- 3 Graduate Studies
- 4 Executive Leadership
- 5 Research Center Management
- 6 Chief of Staff/Protocol and Outreach
- 7 Business Administration
- 8
- 9

Risk Assessment Tools

Excel Worksheets - Risks





Research Development, Programs & Facilitation	IMPACT	PROB.
Decrease in State support	h	h
Lack of research management information	h	m
Ineffective metrics for evaluating programs and personnel	h	m
Lack of seed/incentive funding	h	m
Lack of industrial funding/partnerships	m	h
<u>Research Finance & Administration</u>		
Noncompliance with policies, rules, and laws	h	h
Untimely reporting	h	h
Not rewarding academic excellence	h	h
Lack of coordinated research administration	h	m
Unfunded mandates	h	l
Not following protocols	h	2h

Risk Assessment Tools

Risk Footprint Example

ACTIVITIES	RISKS											
	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

Identify Mitigating Activities

- Mitigating activities include the organizational structure, policies, actions, controls, and procedures that management uses to manage the risks
- Risk assessment includes evaluating the mitigating activities/controls
 - effectiveness and efficiency
 - over- or under-controlled (resource allocation)
 - functioning as intended
 - deficiencies in accountability/responsible person
 - identify gaps

Risk Assessment Tools cont'd

Mitigating Activities Example

		Risks						
Research Finance & Administration		Noncompliance with policies, rules, laws	Untimely reporting	Not rewarding academic excellence	Lack of a coordinated research admin. structure	Unfunded mandates	Not following protocol	Evidence of Control Activity
Mitigating Activities	Training	x	x				x	Grant training for proposal development group, Research Foundation personnel, and dept staff. New faculty orientation. Online training.
	Marketing & communication to Legislators & Public			x		x		Presentation to legislature (Govt. Affairs/VPR/President). Publications/Website. Research road show - committee.
	Policies/Forms				x		x	Cost sharing, review procedures, signed approval documents.
	Signature authority - based on delegation	x	x		x		x	Signature sheets. Email notification for changes.
	PI certifications						x	Online training. Forms signed.
	Office of research compliance	x	x		x		x	Manager oversight and verbal communication with Sr. mgmt
	Budgetary control	x	x		x	x		Budget analysis (budget vs. actual). Analysis review documented by signature and date.

Review Monitoring

- Monitoring processes include higher level reviews to ensure critical mitigating activities are performed on a regular basis.
 - Review that the mitigating activity is done effectively and efficiently and evaluate how management knows things are working as planned (executive management reporting)
 - Review and update, if necessary, the accountable person responsible for the mitigating activity

URC Status Reviews

- Perform a status review following the risk assessment
 - Focus on significant “red” risks
 - Review performed by URC personnel
 - Verify the evidence/documentation that the mitigating procedure/control was effectively done
 - Confirm who the accountable person is responsible for the mitigating activity
 - Review the monitoring, reporting, and any assurances provided to executive management that the significant risks are effectively managed

Enterprise Risk Management

TAMU benefits/positive changes:

- Enhancing capability to identify potential events and establish responses
- Enhancing risk response decisions
- Increasing risk consciousness in decision making
- Identifying and managing cross-enterprise risks and providing integrated responses to multiple risks
- Focusing resources and efforts on key high risk areas
- Improving allocation of resources
- Personnel understanding how mitigating activities/controls affect risks – improves compliance
- Employees being part of the solution and active in identifying and managing risks – improves compliance

University Risk and Compliance (URC) Resources

- Web-sites
 - <http://urc.tamu.edu>
 - Contact information
 - Link to “Risk Management”
 - <http://universityrisk.tamu.edu/>
 - Information about TAMU’s Risk Mgt. Program (ERM)
 - Risk Assessment Tools
 - Excel files and instructions
 - Presentations and other resources

Questions?

