



Council of Senior Business Associates Winter Workshop

**Risk Management
at
Texas A&M University**

**Peggy Zapalac
University Risk and Compliance**

January 8, 2008

ERM at TAMU



- TAMU management supports Enterprise Risk Management (ERM) and the university-wide efforts to identify and manage risk and associated compliance requirements
- TAMU established a University Risk and Compliance office in 2004
 - Began the implementation of 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

A *process applied across the enterprise,*

designed to *identify potential events* that may affect the university and

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

that provides reasonable assurance regarding the *achievement of the university's objectives.*

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 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 risks
 - Limit, avoid, accept, transfer, share
- Monitoring and reporting processes

– Risk assessment

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

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.

Performing a Risk Assessment



Arrange information gathering and meetings with division/dept. head

Meetings typically consists of three 2-hour sessions several days/week apart

Attendees include division/dept head, direct reports, and others (ideal group size depends on unit)

Two person team leads the process - a facilitator and a scribe; unit coordinator

Efficient process includes prep before and homework after meetings

Risk Assessment Steps



Review mission/strategic plan/goals/objectives

Identify activities

Identify and rank risks

Identify and document mitigating activities

Review monitoring and executive reporting
processes

Follow-up with a walk-through review

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 – Risks



Example

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

Research Finance & Administration

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

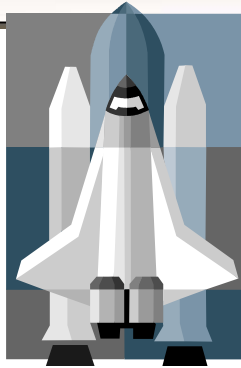
l

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

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



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
M i t i g a t i n g A c t i v i t i e s	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.

Monitoring and Exec. Level Reporting



- Monitoring processes include higher level review and evaluation to ensure that significant mitigating activities
 - are performed on a regular basis;
 - the mitigating activity is effective and efficient;
 - the accountable person is identified and knowledgeable of his/her responsibility; and
 - management knows things are working as planned (executive management reporting).

URC Follow-up



- Perform a walk through review following the risk assessment
 - Focus on significant “red” risks
 - Review performed by URC personnel
 - Confirm who the accountable person is responsible for the mitigating activity
 - Observe the evidence/documentation of the mitigating procedure/control and verify the activity is effective in managing the risk
 - Review the monitoring, reporting, and any assurances provided to executive management used to assist them in effectively managing the significant risks affecting their area

Risk Assessments at TAMU



Risk Assessments

- Risk Management Discussion Group
- Provost
 - URC, EHSD, and UPD
 - College Asst. Deans/SABAs
 - Assessment
 - Information Technology
 - IPO
 - College of Science
 - College of Education
- Research
 - Research Compliance
- Student Affairs
- Athletics
- Athletic Compliance
- Facilities
- Finance (Controller)
 - University-wide financial
 - Transportation Services
 - A/P and A/P Task Force
 - CSBA
 - Student Business Services
 - FMO and TAMUG-FMO
- Communications and Marketing
- Governmental Affairs
- Diversity
- Development
- TAMU Galveston
- TAMU Qatar

Major Risks Facing the University



- Risk of non-compliance w/State, Federal requirements (FERPA, HIPAA, copyrights, intellectual properties, student financial aid, international laws on immigration, etc.)
- Not achieving diversity outcomes that are significant in the eyes of our constituencies (faculty, staff, students).
- Risk associated with community/university perspectives/relationships regarding abuse (verbal, physical, violence) against international students/staff and other diverse groups.
- Risks associated with large scale open events (i.e., conferences, camps, visitors, student groups, the corps of cadets, athletic events, etc.) - open environment.
- Risks associated with not achieving and maintaining a diverse environment in areas of admissions, student recruiting, curriculum, instruction, university sponsored activities, etc.

Major Risks Facing the University



cont'd

- Risks associated with student behaviors (hazing, underage drinking, off-campus bonfire, ring dunking, etc.)
- Risks associated with student travel to University sponsored events.
- Risks related to safety issues that accompany an under trained, overconfident, and youthful constituency.
- Safety and security risks in instructional environments (classrooms, labs, University vessels, instructional & research related fieldwork, use of equipment, co-op/intern assignments, etc.)
- Deteriorating facilities and infrastructure (campus buildings, student housing, physical plant operations, funding repairs/maint., etc.)
- Inability to change safety culture (reporting, training, corrective actions on & off campus, etc.)

Major Risks Facing the University



cont'd

- Reduced funding combined with an anticipated growth factor (Inability to generate adequate additional revenue)
- Risk of implementing large scale improvements to IT infrastructure (EIS project, etc.)
- Risks associated with Info Technology failures (loss of systems, loss of data, theft of data, intrusions/malware, obsolescence, confidential/sensitive data, etc.)
- The inability to effectively demonstrate the diverse funding issues and roles of various institutions of higher education at the state level
- Noncompliance in research activities (conflicts of interest, research misconduct, etc.)

Hot Audit, Risk, and Compliance Topics



Current Audit, Risk, and Compliance Issues

- Governance
- Safety
- Compliance
- Monitoring

Governance

- Mission, goals and objectives, strategic plans
 - Performance measures
 - University procedures
 - Rules and SAPs
 - Written procedures
 - Succession planning
 - Risk management

Safety



- Safety Program
 - Training (safety champions)
 - Safety committees (oversight, lab safety, fieldwork safety)
 - Safety training standards (safety manual, lab manuals)
 - Safety Hotline [<http://safetyhotline.tamu.edu/>]
- Business Continuity and Disaster Recovery
 - Planning for disasters, open campus events
 - Emergency Preparedness [www.tamu.edu/emergency], Task Force on Campus Emergencies, Code Maroon
- Risk and Misconduct Hotline (Ethics Point)
 - Implementation March 2008
 - System steering committee
- Camps and Enrichment Programs
 - Types of activities, waivers, insurance, personnel screening [Rule 11.99.99.M1]

Compliance



- Security of sensitive/confidential information and privacy concerns
 - FERPA, HIPPA (email, phone calls, hard copies)
[University Rule 13.02.99.M1]; See University's FERPA policy at <http://admissions.tamu.edu/Registrar/General/FERPA.aspx>
 - Portable computing devices (laptops, jump drives, etc.)
[University Sap 24.99.99.M1.16]
 - Personal information (personal files, payroll, checks, etc.)
[University SAP 24.99.99.M1.24, Sensitive Personal Information]
- Conflict of Interest [System Policy 07.01]
- Effort Reporting
- External reporting (Accuracy, Integrity, Timeliness)

Monitoring



- Executive, supervisory, and operational levels
 - Contracts [University Rules 25.07.99.M1 and 25.07.99.M2]
 - Procards and accounts payable
 - Continuing education
 - Account reconciliations/verifications
 - Segregation of duties
 - Revenues – cash handling, accounts receivable
 - Disbursements – receiving, approving

Questions?



University Risk and Compliance Web Pages:

<http://urc.tamu.edu>

- Contact information
- Link to Risk Management
- Link to Compliance
- Link to TAMU Rules/SAPs

<http://universityrisk.tamu.edu/>

- ERM Information
- Risk Assessment Tools
 - Excel files and instructions
 - Risk dictionary
- Presentations

<http://compliance.tamu.edu/>

- Code of Conduct