

Texas A&M University

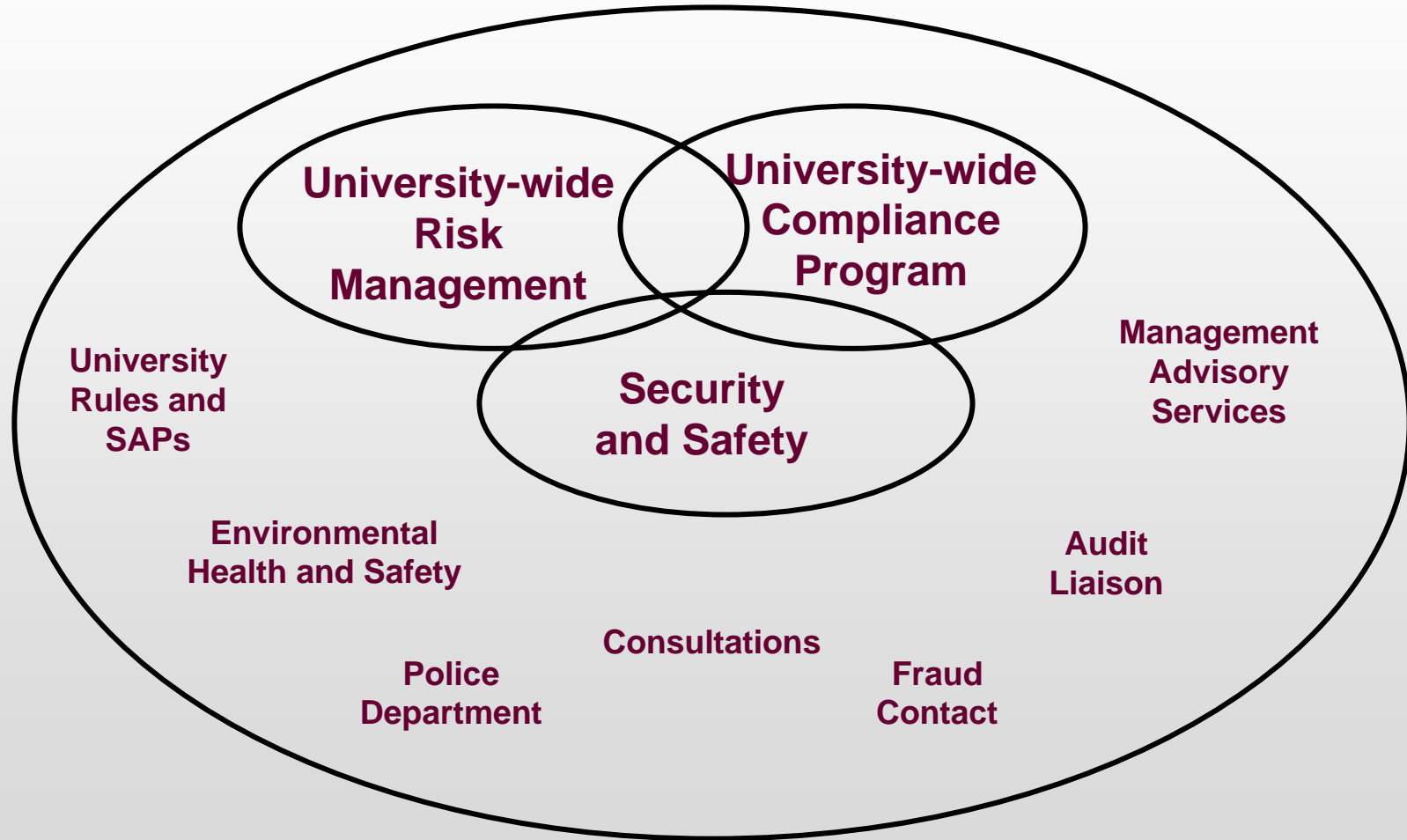
University-wide Risk Management and University-wide Compliance

**CSBA Monthly Meeting
July 20, 2005**

University Risk and Compliance Office

- The University Risk and Compliance Office was established in April 2004
- Responsibilities of URC include:
 - Implementing enterprise risk management
 - Implementing university-wide compliance program
 - Coordinating established areas and responsibilities
 - Environmental Health and Safety
 - Rules and SAPs
 - Management Advisory Services
 - Police Department
 - Audit Liaison and Fraud Contact

University Risk and Compliance Office



Enterprise Risk Management

University-wide Risk Management Program

Mission: To integrate an enterprise-wide risk management process within the University designed to identify and assess risks and the risk management strategies used to provide reasonable assurance regarding the achievement of the University's objectives

University-wide Risk Management Components

- Support from the top
- Involvement of personnel at all levels
- Perform risk assessments
 - Identify risks (brainstorming)
 - Rank risks (probability and impact)
- Identify mitigating activities
 - Actions, procedures, and processes used to manage risks (limit, avoid, accept, share)
 - Identify accountable/responsible person/position
 - Duties are known and periodically evaluated
- Report results and any gaps to the President and Provost
- On-going monitoring
- Performing self-assessments

University-wide Risk Management Implementation Strategy

- Introduce the University-wide risk management program and establish a common risk language
 - Definition of risk
 - Any event or action that adversely impacts the University's ability to achieve its objectives
 - Risk categories
 - Strategic, operational, reputational, financial, and compliance
 - Risk ranking (high, medium, low)

Risk Categories

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 loss of assets, technology risks, etc.)

Operational

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

University-wide Risk Management Implementation Strategy

- Risk Assessments
 - Identify risks and build a portfolio of risks
 - Input from representatives within the University
 - Peer institutions (web sites/list serves)
 - Training seminars/conferences
 - State auditors
 - COSO and other publications
 - Analyze and assess risks
 - Prioritize and rank (high, medium, low)
 - Probability of occurrence (likelihood of happening)
 - Potential impact (consequences)

Levels of Control in COSO

Collaborative Assurance

(Governance and Management Control Processes)

I-----I

← Periodic Assurance →
(Governance Control Processes)

I-----I

I----- On-going Assurance -----I

(Management Control Processes)

Level 1
Controls
(Execution)

Level 2
Controls
(Supervisory)

Level 3
Controls
(Oversight)

Level 4
Controls
(Int/Ext Audit)

During
execution of
event or
transaction

Immediately
after execution
of event or
transaction

Soon after
execution of
event or
transaction

Pre and post-
operations audit of
execution of on-
going assurance

University-wide Risk Management

Level 1 Controls

(Execution Activities/Controls)

- Embedded in day-to-day operations
 - Policies and procedures
 - Segregation of duties
 - Comparisons and reconciliations
- Performed on every event/transaction
- Performed by the generators of the event/transaction
- Performed in ‘real time’, as the event/transaction is executed

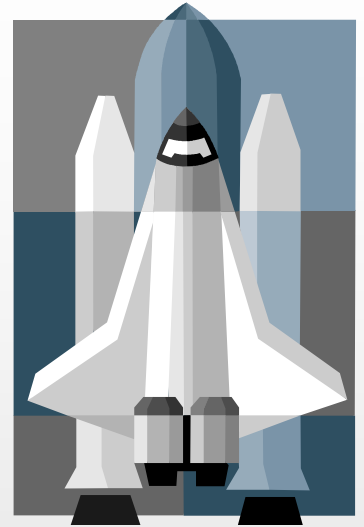
University-wide Risk Management

Level 2 and **Level 3** **(Supervision)** **(Oversight)**

- Monitoring of the operations
 - Review policies and procedures
 - Assess segregation of duties
 - Review and sign-off of reconciliations
- Performed on most or a sample
- Performed by a co-worker, supervisor, or manager of the event/transaction
- Performed after the fact, following the event/transaction
- Trend analysis and high level review

University-wide Risk Management

Ranking the Risks



Impact - *the effect on achievement of objectives, the consequence(s)*

High

showstopper, significant injury or death, large loss, loss of program, criminal penalty, liability

Medium

inefficient and extra work, fines, minor injury, moderate loss

Low

little to no effect, warning, reprimand

University-wide Risk Management

Ranking the Risks

Probability - *the likelihood of the risk happening*



High will happen frequently, occurs often, predictable

Medium will happen infrequently, sometimes occurs, unpredictable

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

University-wide Risk Management Risk Footprint Example

#	ACTIVITIES	RISKS →																	
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15			
3	Administration (13, 15, 18, 23)	HH	Bad PR	HH	Fraud	HH	Staff turnover	HM	Lawsuit-class action	HL	Contractor goes bankrupt	MM	Failure to comply with rules, regs, etc.	MM	Inability to recruit qualified staff	MM	Lack of performance by contractor	MM	Operation budget shortages
2	Facility (5, 6, 7, 12, 19, 20, 21, 22)	HM	Inadequate communications system	HM	Inadequate space	HM	Unhealthy environment	MM	Equipment failure	ML	Poor lighting	ML	Power failure	ML	Unsafe building	LM	Lack of sufficient storage	LM	Unsafe furniture
1	Security & Safety (2, 3, 4, 8, 11, 14, 16, 17)	HM	Lack of ER training	HM	Lack of trained security	HL	Failure to comply with regs., laws	HL	Fire & acts of nature	HL	Lack of plan or Failure to	HL	Riot	MM	Physical attack	MM	Vandalism	ML	Death
4	Maintenance (1, 7, 9, 10)	HM	Insecure facility	HM	Unlicensed facility	MH	Deferred maintenance	MM	Equipment breakdown	MM	Inadequate staff	MM	Theft	MM	Unsanitary or unhealthy environment	ML	Injury or death	LM	Lawsuit - individual

University-wide Risk Management Mitigating Activities

- Identify mitigating activities
 - The University’s organization, policies, and procedures used to reasonably ensure that:
 - Programs achieve their intended results consistent with the University’s mission
 - Programs and resources are protected from waste, fraud, and mismanagement
 - Laws and regulations are followed
 - Reliable and timely information is obtained, maintained, reported, and used for decision making

University-wide Risk Management

Evaluate Mitigating Activities

- Evaluate the mitigating activities identified
 - Review activities where two or more are identified as the responsible person
 - Review activities for effectiveness
 - Review if resources are appropriately allocated based on the level of risk and desired level of effectiveness

University-wide Risk Management

Evaluate and Monitor Results

- Identify gaps in the mitigating activities, if any
 - Faulty underlying processes/procedures
 - Deficiencies in areas of accountability
 - Review the costs and effectiveness of the mitigating activities relative to the risk ranking
- Create a monitoring plan that addresses all critical risks identified (accountable person)
 - Correlate Level 2 and Level 3 controls with the appropriate Level 1 controls
 - Identify and document the evidence that the procedure/control was done

University-wide Risk Management Implementation Tools

- Excel spreadsheets
 - Linked with macros
 - Free (developed by David B. Crawford, UT)
- Optionpower voting software and touch pad equipment
 - Anonymous ranking of impact and probability

University-wide Risk Management Implementation at TAMU

- Begin at high level
 - Formed Risk Management Discussion Group
 - Members include positions with direct reporting relationship to the President or Provost
 - Actions of Risk Management Discussion Group
 - Identified major risks facing the University
 - Identified mitigating activities for the top risks (high/high)
 - Identified accountable/responsible person or position for the top risks

University-wide Risk Management Implementation Strategy

- Perform risk assessments on the major areas of the University such as:
 - President's Office
 - Provost's Office
 - Research
 - Student Affairs
 - Athletics
 - Athletic Compliance
 - Facilities
 - Finance
 - Governmental Affairs
 - Faculty Senate
 - Communications
 - Assessment and Diversity
 - Development

Compliance Areas

(not all inclusive)

- Health and Safety
 - EPA, FAA, CDC
 - Clery Act
- Privacy
 - FERPA
 - HIPPA
 - Gramm Leach Bliley
- Research misconduct
- Research Integrity
 - Human, Animal, Biosafety
- Grant/contract management
- Drug free workplace
- Labor laws
- ADA
- Financial reporting
- Procurement
- Tax codes
- Record management
- Patriot Act
- Immigration (SEVIS)
- Export
- Controlled substances
- NCAA

University-wide Compliance Program

_____Focus_____

Accountability

Excellence

Coordination

Training

Due Diligence

Human Factor

Communication

Interactive Process

Ethics as Norm

Commitment

Collaboration

Shared Responsibility

University-wide Compliance Program

Mission: Develop and maintain an effective, proactive, compliance program aligned with the University's strategic goals to:

- Promote and support a culture that requires accountability;
- Demonstrate commitment and due diligence to deter and detect compliance violations; and
- Expect compliance and ethical conduct as the norm.

Compliance Program Framework

(Based on Federal Sentencing Guidelines)

- Effective Compliance Program Requirements
 - Assign overall program coordination at high level with direct access to executive management
 - Have standards to deter and detect misconduct (i.e., formal policies and rules, network of compliance expertise)
 - Care in delegation of authority (demonstrate integrity and ethical conduct)

Compliance Program Framework

(Based on Federal Sentencing Guidelines)

- **Effective Compliance Program Requirements**

(Continued)

- Provide on-going education and training
- Monitor, assess, and provide system for employees to report or seek guidance on compliance issues without fear of retaliation
- Enforce consistently and use appropriate discipline and incentives
- Periodically assess program effectiveness and report compliance status to executive management

University-wide Risk Management and University-wide Compliance Challenges

- Changing the environment – keeping the momentum
- What to do with the information
- Time and resources

University Risk and Compliance Contacts

- Charley B. Clark, Associate Vice President of University Risk and Compliance
cbc@tamu.edu, 845-0977
- Margaret “Peggy” Zapalac, Director of University Risk Management,
m-zapalac@tamu.edu, 845-8115
- Annette C. Wallis, Director of University Compliance
a-wallis@tamu.edu, 862-7737