

Texas Engineering Extension Service

Enterprise Risk Management

**ERM Retreat
August 10, 2005**

Enterprise Risk Management

Definition: A process applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within the entity's risk appetite, to provide reasonable assurance regarding the achievement of the entity's objectives

Enterprise Risk Management

ERM encompasses:

- Aligning risk appetite and strategy
- Enhancing risk response decisions
- Reducing operational surprises and losses by enhancing capability to identify potential events and establish responses
- Identifying and managing cross-enterprise risks
- Providing integrated responses to multiple risks
- Identifying events representing opportunity
- Improving allocation of resources

Enterprise Risk Management Components

- Support from the top
 - Involvement of all levels of personnel
- Risk assessments
 - Identify risks (brainstorming)
 - Rank risks (probability and impact)
- Mitigating activities
 - Actions, procedures, and processes used to manage risks (limit, avoid, accept, transfer, share)
- Monitoring plan
- Report results and any gaps
- On-going

Enterprise Risk Management Implementation Strategy

- Introduce enterprise risk management to the organization
- Establish a common risk language
 - Definition of risk
 - Any event or action that adversely impacts the organization's ability to achieve its objectives
 - Risk categories
 - Strategic, operational, reputational, financial, and compliance
 - Risk ranking
 - High, medium, low
 - Numerical

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

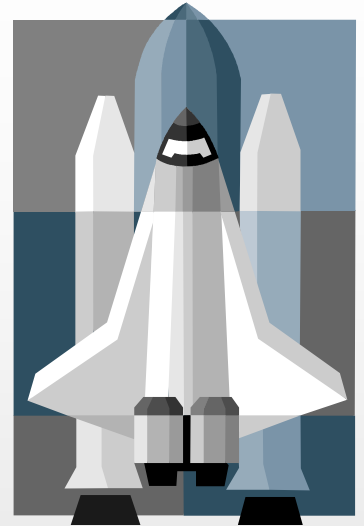
(affects on-going management processes and procedures, etc.)

Enterprise Risk Management Implementation Strategy

- Risk Assessments
 - Identify major activities/processes/functions
 - Identify risks and build a risk portfolio
 - Representatives within the organization
 - Peer institutions (web sites/list serves)
 - Training seminars/conferences
 - Auditors – state, system, external
 - COSO and other publications
 - Analyze and assess risks
 - Prioritize and rank (high, medium, low; numerical)
 - Consider probability of occurrence (likelihood of happening)
 - Consider potential impact (consequences)

Enterprise 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

Enterprise Risk Management

Ranking the Risks

Probability - *the likelihood of the risk happening* (consider level 1 controls)



High will happen frequently, occurs often, predictable

Medium will happen infrequently, sometimes occurs, unpredictable

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

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 assurance¹⁰

Enterprise 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

Enterprise Risk Management

Level 2 Controls and Level 3 Controls

(Supervision)

- Re-application of operating controls
 - Supervisory Review; Quality Assurance; Self Assessment
- Performed very soon after the generation of the event/transaction
- Performed by line management or staff positions who do not originate the event/transaction
- Performed on a sample of the total number of events/transactions

(Oversight)

- Exception reports, status reports, analytical reviews, variance analysis
- Performed by representatives of executive management
- Performed on information provided by supervisory management
- Performed within a short period (weeks/months) after the event/transaction is originated

Enterprise Risk Management

Level 4 Controls (Internal/External Audit)

- Audit of the design of controls not the operation of controls
- Performed either before the event/transaction is originated or long after
- Performed by staff with no involvement in the operations
- Performed on individual events/transactions for discovery only

Enterprise Risk Management

Risk Assessment Steps

- Identify activities, processes, functions
- Identify risks related to the activities
- Rank the risks identified
- Develop a risk footprint
 - Grid of risks that is color coded based on the ranking

Enterprise Risk Management

Risk Footprint Example

#	ACTIVITIES	RISKS →															
		1	2	3	4	6	7	8	9								
3	Administration (13, 15, 18, 23)	HH	Bad PR	HH	Fraud	HH	Staff turnover	HM	Lawsuit-class action	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	H M	Unhealthy environment	M M	Equipment failure	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	Riot	MM	Physical attack	MM	Vandalism	ML	Death
4	Maintenance (1, 7, 9, 10)	HM	Insecure facility	HM	Unlicensed facility	M H	Deferred maintenance	M M	Equipment breakdown	MM	Theft	MM	Unsanitary or unhealthy environment	ML	Injury or death	LM	Lawsuit - individual

HH, HM = Extensive risk management and considerable risk management (all levels of control)

HL, MH = Manage and monitor (all levels of control)

MM, ML, LH = Monitor (only execution controls and supervisory controls)

LM, LL = Accept (accept the risk and have little or no controls)

Enterprise Risk Management

Mitigating Activities

- Mitigating activities are the entity's organizational structure, policies, and procedures
 - Used to reasonably ensure that:
 - Programs achieve their intended results consistent with the entity'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

Enterprise Risk Management

Identify Mitigating Activities

- Identify mitigating activities for each risk
- 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 controls
- 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

Enterprise Risk Management

Evaluate and Monitor Results

- Create a monitoring plan that addresses all critical risks identified
 - Identify the accountable person responsible for the mitigating activity
 - Identify and document the evidence that the procedure/control was done
 - Correlate Level 2 and Level 3 controls with the appropriate Level 1 controls

Enterprise Risk Management

Mitigating Activities/Control Footprint

Level	Maintenance (1, 7, 9, 10)	Insecure facility	Unlicensed facility	Deferred maintenance	Equipment break down	Inadequate staff	Theft	Unsanitary or unhealthy environment	Injury or death	Lawsuit - individual
3	Mgr. Walkthrough	x	x		x		x	x	x	x
1	Security check on staff ins & outs	x					x		x	
1	Preventive maintenance schedule	x	x	x	x			x	x	x
2	Supervisor reviews completed maintenance	x	x	x	x			x	x	x
3	Spot check of equipment by Mgr.	x	x	x	x			x	x	x
1	Checklist of tasks		x					x	x	x
2	Visual inspection by Supervisor		x					x	x	x
1	Training of employees	x	x		x	x	x	x	x	x
2	Comparison of training log to list of employees	x	x		x	x	x	x	x	x
3	Exception report to Mgr. About emps not attended	x	x		x	x	x	x	x	x

Enterprise Risk Management

Monitoring Plan

Maintenance (1, 7, 9, 10)	Operating (Level 1) Control	Evidence of Operating(1) Control	Supervisory (Level 2) Control	Evidence of Supervisory(2) Control	Oversight (Level 3) Control	Evidence of Oversight(3) Control
Insecure facility					Mgr. Walkthrough	Memo of exceptions noted in walkthrough and actions taken; signed and dated
Unlicensed facility	Preventive maintenance schedule	Preventive maintenance schedule	Supervisor reviews completed maintenance	Supr. Signs & dates report with notes	Spot check of equipment by Mgr.	List of equip. checked; Memo to file; Sign log on equip.
	Training of employees	Training roster, certificates, curriculum	Comparison of training log to list of employees	Report of exceptions signed and dated	Exception report to Mgr. About emps not attended	Manager initials and dates with comments of actions taken
	Checklist of tasks	Completed checklist signed & dated by employee performing task	Supervisor verifies & signs checklist	Memo or notes on exceptions noted and actions taken; signed and dated		
	Security check on staff ins & outs	Log of ins and outs that failed security check; signed by security				

Enterprise Risk Management Challenges

- Getting started
- Common language
- Changing the environment/culture
- What to do with the information
- Continuous process- keeping the momentum
- Time and resources

Enterprise Risk Management

- Questions
- Contact Information
 - Margaret “Peggy” Zapalac, Director of University Risk Management
 - m-zapalac@tamu.edu
 - 845-8115