The Texas A&M University System Enterprise Risk Management Reference

To be used as a reference by Members when

developing respective ERM Program

Developed by System Risk Management
Contact: Henry D. Judah, CPCU CLU ChFC or Risk Management Coordinator Charles Longoria
August 29, 2012

Introduction

- Events such as management changes and reorganizations, demands for increased accountability by funding sources and new legislation have heightened the awareness of the various risks facing the university community.

- The course will introduce the basis concepts of Enterprise Risk Management (ERM) and provide a core program for System members to use when working through the ERM process

System ERM Course Objectives

- At the conclusion of this presentation, you will be able to:
  - Define important Enterprise Risk Management terms and activities
  - Describe the reporting process
  - Identify and apply the major steps of the Enterprise Risk Management process

What is Risk?

- Various Definitions of Risk:
  - Possibility of loss or injury; peril
  - The International Organization for Standardization (ISO) Guide 73, Risk Management, has defined risk as the combination of the probability of an event and its consequences.
  - Possibility that taking action or the lack of action could adversely affect the ability to achieve strategic goals and operational objectives.

Risk and Risk Management

- In all activities, there is the potential for events and consequences that may result in opportunities for benefits or threats to success, particularly as it relates to strategic objectives.

- The key is to decide if an activity should be undertaken or avoided based on whether the probability of a positive outcome outweighs the probability of a negative consequence in the activity. This in essence is the decision process of risk management.

Risk Management Defined

- Traditionally, business has considered risk primarily as a personnel safety or financial loss issue and has focused on the mitigation of the negative consequences.

- For the success of any organization, both the positive and the negative aspects of risk must be considered.

- Enterprise Risk Management is the process used to methodically address risk with the goal of achieving sustained benefit to the organization and the minimization of negative consequences to the organization.

Risk Management Defined

- All this is done in direct relation to the institutional mission of the organization and the strategic objectives established to fulfill the mission.

- The application of this process within an institution is known as the Enterprise Risk Management Process (ERM)

Enterprise Risk Management

- Enterprise Risk Management (ERM) is a process-driven tool enabling management to visualize, assess, and manage significant risk.

- ERM can be described as a risk-based, intentional approach to assigning the likelihood and severity of risk which could prevent the attainment of the strategic goals of the member.

ERM Process

- The Risk Management Assessment (RMA) is a process used to identify, quantify, evaluate and treat risk to the member.

- The process starts with a review of the member's strategic objectives and then uses a systematic review process to identify and manage risks which could impact the successful attainment of the strategic objectives.

Risk Management Assessment Cycle

- Review Strategic Objectives
- Perform Risk Assessment
- Evaluate Risk
- Treat Risk
- Monitor Risk Mitigation Process

Review Strategic Objectives

- A review of the member's strategic objectives is performed to identify what actions must be taken for the member to succeed.
- Effective performance of this step requires knowledge of the member and the context within which the member operates.
- An important outcome of this review is the identification of the "owner" of each objective or the department, personnel or person who is responsible for its success.
- That group or person is then assigned to perform the risk review for that objective.

Perform Risk Assessment

- Now that the key strategic objectives are identified and assigned, it is important to complete a Risk Assessment. The first step in the assessment process is the risk analysis phase.

- This includes:
  - Identification
  - Description
  - Estimation

- Each of these sub-steps will be reviewed

Risk Identification

- The purpose of risk identification is to identity the member's exposure to events that prevent it from reaching its strategic goals. It should include:
  - List of threats or risk
  - Areas where the member may exploit for competitive advantage

- Effective risk identification helps the member:
  - Document and compile a comprehensive list of risks
  - Determine scope of risks
  - Categorize risks

Categories of Potential Risks

- **Strategic Risk/ Operational Risk** -These concern the long-term strategic risks of the organization such as capital availability, political risks, regulatory changes and reputation.

- **Financial Risk** - These concern the effective management and control of the finances of the member. For state higher education institutions, this is likely centered on legislative funding, federal student aid funding and research grant funding.

- **Compliance Risk**-These concern the adherence to applicable laws and regulations, both internal and external. This category of risk is supported and monitored via the System Ethics and Compliance Officer and program.

- **Reputational Risk:**-Any risk that affects public perception and reputation.

- **Hazard Risk-** These concern factors such as liability suits, theft, personal injury and business interruptions.

Driving Factors of Potential Risks

- There may be more than one potential risk category and the probability and severity for each category should be addressed during the risk analysis.
  - It is recommended to use a probability and severity risk rating. High, Medium, and Low ratings should be assigned to probability and severity areas.
  - The member should only be concerned, for the purposes of the ERM process, for those risk that either have a high/high, high/medium, medium/high and medium/medium probability/severity rating.
  - See sample table

Risk Identification Techniques

- The objective of these techniques is to gain a better understanding of where and what areas pose a threat to the success of the member's strategic objectives.

- Example identification techniques include:
  - Brainstorming
  - Questionnaires
  - Scenario Analysis
  - Risk Assessment Workshops
  - Incident Investigation
  - Auditing and Inspection
  - Industry Brainstorming

Risk Description

- The next step is to organize the high/high, high/medium/, medium/high and medium/medium risks in a formal and organized manner. The risk description should be brief but include sufficient information to allow the member to prioritize and assess each risk in relation to:

  - Scope-qualitative description of the potential event (size, type, number and dependencies
  - Nature-strategic, operational, financial, hazard or compliance
  - Stakeholders-public, students, faculty, staff
  - Risk Tolerance-ability/importance to survive the risk of it occurs

Risk Description Continued

- Risk mitigation and control mechanisms-how to control the likelihood and/or severity if a risk occurs
- Action Plans-plans on how to minimize both severity and likelihood of risk occurring
- Strategy and policy development-who will develop actions plans to minimize the likelihood/severity of risk and monitor the plan over the course of the year
- See sample matrix

Risk Evaluation

- The risk evaluation is used to make decisions about the significance of risks to the strategic goals of the member and whether each specific risks should be accepted or treated

.

- As outlined, only those risks rated as high/high, medium/high, high medium and medium/medium should be included in the ERM process.

- Those risks lower in either severity or likelihood should be evaluate and mitigated, however those mitigation activities should be handled with the appropriate level of administration for the particular area.

- The risk evaluation may result in a decision to accept the potential for a negative outcome due to a low probability or severity of an occurrence.

Risk Mitigation

- Risk mitigation is the process of selecting and implementing measures to modify or mitigate risk. Any risk mitigation process should:
  - Be effective and efficient in operation
  - Possess effective internal controls
  - Be in compliance with laws and regulations

- Effectiveness relates the cost of implementing the control to the risk reduction benefits expected. Additionally, the potential economic effect if no action is taken versus the cost of proposed action must be considered. The responsible part of the risk mitigation strategy should develop a risk mitigation plan to provide a framework for implementing, monitoring and reporting actions put in place to mitigate the risk.

Risk Mitigation Plan

- The Risk Mitigation Plan is developed as a result of the Risk Assessment process. It defines how the risk is to be addressed within the ERM process

- Again, the ERM Risk Mitigation Plan should focus on those risks that could impact the strategic goals of the Member that have a high/high, medium/high, high/medium and medium/medium rating for probability/severity.

Options To Treat Risk

- Accept the risk (risk deemed acceptable, compared to the cost of improving controls to mitigate)
- Implement a suitable control strategy using controls to reduce the risk
- Avoid the risk (don't do the activity)
- Transfer the risk to another entity (insurance company, via contractual transfer etc)

ERM Monitoring and Follow-up

- After completion of the ERM process and the development of action plans to mitigate risk, members must observe and monitor those operations to determine if the prescribed action plans are implemented, monitored and measured.

- The assigned department responsible for the action plan should report at regular intervals to the ERM Committee about their ongoing management of the risk

Suggested Enterprise Risk Management Structure

- The institutional body responsible for the overall implementation and monitoring of the ERM process should be the member's Executive Committee.

- Direct reporting to the president or agency director by the Executive Committee is critical for an effective ERM process.

ERM and Compliance-Working Together

- Compliance is one area of a complete ERM Program

- Member's have the option of placing the ERM process within the System Ethics and Compliance Committee as outlined in System Policy 16.01 System Ethics and Compliance Program and System Regulation16.01.01 System Ethics and Compliance for ease of management and elimination of redundancy.

Enterprise Risk Management System Policy

- The Strategic Planning Framework of System Policy 03.01 includes System Mission, Vision, Core Values and Strategic Planning Policy. The ERM process provides the mechanism to identify risks which may impact each of these components

- It states: “Enterprise Risk Management assesses and defines actions to be taken by the system members, the System Offices, and/or the system to identify, monitor, and mitigate risks that threaten the achievement of strategic plan goals and/or continuing operational programs.”

Summary

- ERM is a management tool used to positively change culture
- Risk Management is part of an organization's strategic plan that benefits and compliments the successful pursuit of the member's strategic objectives.
- ERM is a continuous process of identifying, analyzing, prioritizing and assessing, treating and monitoring risks.

Suggested ERM Timeline

- **September**: Begin collection of information on high/high, high/medium, medium/high and medium/medium risks from across the institution/agency.

- **November:** Identified risks are presented to Executive Leadership for review and approval of inclusion on institutional risk matrix

- **End of November:** Submit member risk matrix to System Risk Management

- **January:** Follow up action taken on a quarterly basis through the calendar year to monitor and management risk mitigation activities.

ERM Staff Roles And Responsibilities

Executive CEO

- Oversees the development and implementation of the Risk Management Plan;
- Ensures the ongoing review of risks and updates the Register of Major Risks as needed;
- Encourages a management climate which is aware of and supports risk management; and
- Oversees development of processes to define and address new risks.

ERM Staff Roles And Responsibilities

Risk Management/Executive Compliance Committee

- Coordinates, on an ongoing basis, the implementation of the Risk Management Plan;
- Reviews Risk Matrix and reports to the CEO on recommended changes;
- Regularly convenes the Executive Committee to discuss the Register of Major Risks and necessary changes to that register; and
- Develops and implements risk management procedures and training as needed.

ERM Staff Roles And Responsibilities

Department Heads

- Ensure that risk management controls and processes are included in all planning and research;
- Encourage an organizational climate that supports risk management;
- Ensure that employees understand the importance and consequences of risk management issues in their immediate work areas
- Identify any new risks and report them to an Executive committee member.

References

- System Policy 03.01 System Mission, Vision, Core Values and Strategic Planning
- System Policy 16.01 System Ethics and Compliance Program
- System Regulation 16.01.01 System Ethics and Compliance