Enterprise Risk Management

Why it Really Does Matter

Stewart Citroen

Actuaries Club of the Southwest
Austin, Texas
June 2006

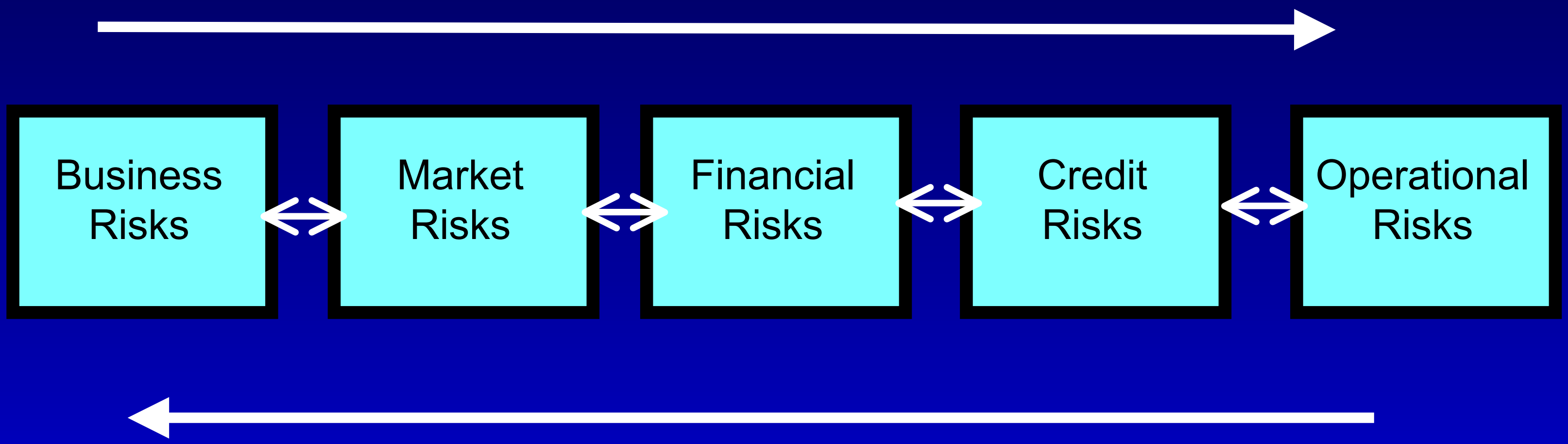
Agenda

- What is Enterprise Risk Management (ERM)?
- How is ERM implemented
- Internal and External Pressures
- Success Factors

Historically, risk typically managed in silos

Business Risks | Market Risks | Financial Risks | Credit Risks | Operational Risks

ERM provides a consistent framework for looking at risks and their interrelationships across the organization



Positive vs. Negative Approach to Risk and Capital Management

Historically, risk management meant saying ‘No’ a lot..

No! We need to focus on risk mitigation.

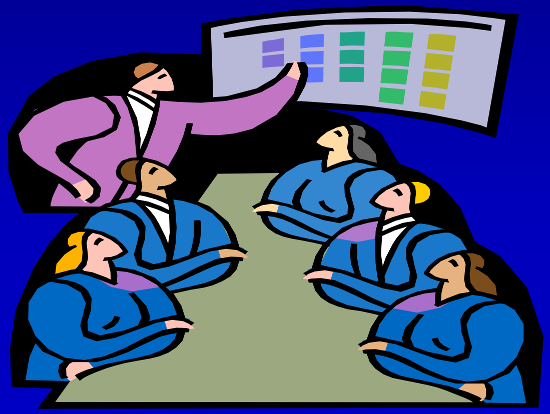
ERM looks at the strategic, upside opportunities

How can we gain a competitive advantage?

Distributed Risk Management vs. Central Risk Oversight

Historically, specific risk expert managing each risk independently

ERM facilitation: specific roles, responsibilities and structures



ERM Definitions

- No single definition
- Committee of Sponsoring Organizations (COSO) definition
  - The American Institute of Certified Public Accountants (AICPA)
  - The American Accounting Association
  - The Institute of Internal Auditors
  - The Institute of Management Accountants
  - The Financial Executives Institute
- Casualty Actuarial Society (CAS) definition

ERM Definitions

COSO Definition

"ERM is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

ERM Definitions

CAS Definition

"ERM is the discipline by which an organization in any industry assesses, controls, exploits, finances and monitors risks from all sources for the purpose of increasing the organization's short and long term value to its stakeholders."

How ERM is Implemented

- Multiple methodologies and frameworks – not a "one size fits all" process
- Basic chronology:
  - Identify
  - Quantify
  - Solve
  - Execute

How ERM is Implemented

Identify

- Include all key exposures
- Continuous process - <u>not</u> a one-time event
- Broad participation – all areas, all levels
- Expose risk interdependencies, hidden risks
- Risk Classification
  - 4 common risk categories:
    Hazard, Financial, Operational and Strategic
  - Risk attributes: sources, events, consequences etc

How ERM is Implemented

Quantify

- Do not need to quantify all risks
- Focus on risks that have biggest influence on ability to achieve strategic goals

Tactical Risks	Strategic Risks
■ Known environment ■ Capabilities and resources on hand to address ■ Low financial impact ■ Requires little or no investment to address risk	■ Unknown environment ■ Not well understood ■ Not well equipped to address ■ Significant financial impact ■ Significant investment needed to address risk

How ERM is Implemented

Quantify

- Scenario planning
  - Identify range and likelihood of outcomes
- Risk models
- Major challenges
  - Lack of data
  - Unstructured risks
- Economic capital

How ERM is Implemented

Solve

- Risk appetite and risk tolerance
  - What risks does the organization want to take?
  - What risks does the organization not want to take?
- Develop action plans for risk profile
- 4 risk responses
  - Accept
  - Avoid
  - Transfer
  - Mitigate

How ERM is Implemented

Execute

- Assign responsibilities
- Monitor risks
- Ongoing, continuous process
- Clear and effective communication and reporting
  - Board
  - Stakeholders
  - Regulators
  - Rating agencies

Internal and External Pressures

- Regulation
  - Basel II Accord
  - Solvency II
  - Sarbanes-Oxley
  - NY Stock Exchange Requirements
  - COSO Framework
- Rating Agencies
  - Evaluating ERM structure and capabilities
  - Looking at Economic Capital models
  - Assessing risk models relative to insurers risks
  - Assessing processes that use information from risk models

Economic Capital (EC)

Europe: Solvency II proposals

U.S: capital and reserving requirements

EC is defined as "*sufficient surplus to cover potential losses at a given tolerance level*"

EC vs. regulatory and rating agency capital

ERM should drive EC models

Internal and External Pressures

- Public demanding better risk management and more accountability
- Corporate governance
  - Board wants assurance risk is being managed
  - Board and senior executives concerned about personal liability
- Shareholder demands for:
  - Financial stability
  - Improved financial performance
- Reputation
  - News reports and perceptions

Success Factors

- Support and involvement of board members and senior management
- Sufficient resources
- Assigned accountability
- Risk-aware culture
  - Clarity and common understanding of ERM
  - Training and education
- Ongoing, continuous behavior