COLLEGE OF MANAGEMENT
NC STATE UNIVERSITY

Welcome to NC State's Enterprise Risk Management Roundtable

"Board of Director Expectations for Enterprise Risk Management"

March 19, 2004

Increasing Calls for Management of Risks

- Among the **core responsibilities of the board** are understanding the issues forces and **risks** that define and drive the company's business
  - *The Conference Board 2003*
- The **audit committee** should understand the corporation's **risk profile** and oversee the corporation's **risk assessment** and management practices.
  - *The Business Roundtable 2002*
- Management required to certify they have programs and controls to **disclose** developments and **risks** pertaining to business
  - Securities and Exchange Commission Final Rules 2003

Increasing Calls for Management of Risks

- 73% of directors support increasing **audit committee's** responsibility for **risks**
- 43% of directors believe they cannot effectively identify, safeguard against, and plan for key **risks**
  - *McKinsey Survey May 2002*
- **Audit committees** should define and use timely, focused information that is responsive to important performance measures and to the **key risks** they oversee
- **Audit committees** should develop an agenda that includes a **periodic review of risk** by each significant business unit.
  - *National Association of Corporate Directors 1999*

Fortune 100 Audit Committee Disclosures About Risk Management

- 69 of 100 ACs involved some form
  - 16 review policies and guidelines only
  - 17 look at policies and lists of business risk exposures
  - 20 look at policies and lists of financial risks only
  - 9 look just at lists of business risks
  - 7 look just at lists of financial risks

Recent CEO Survey Re: Risk Management

- 76% of CEOs somewhat agree or strongly agree that ERM is a priority of the board
- 81% claim they report their company's ERM portfolio to the board

Reaching Common Ground

What is your definition of the term – *Risk?*

Is “risk” all bad?

One of the Challenges

When I say

"*risk management*,"

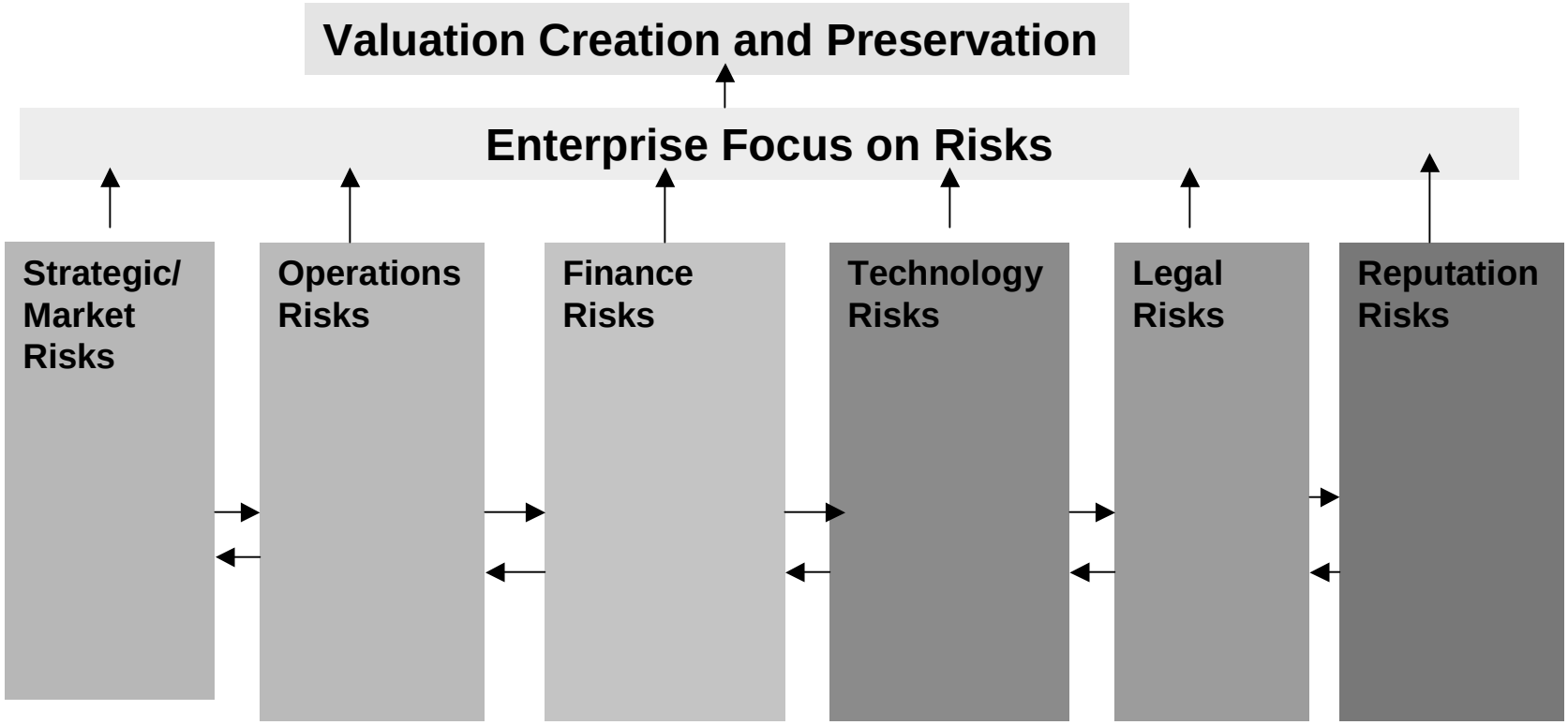
what is the first thing that comes to mind?

COSO's Definition of Enterprise Risk Management

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, manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

- Proposed by COSO (2003)

ERM Brings Together All Risks



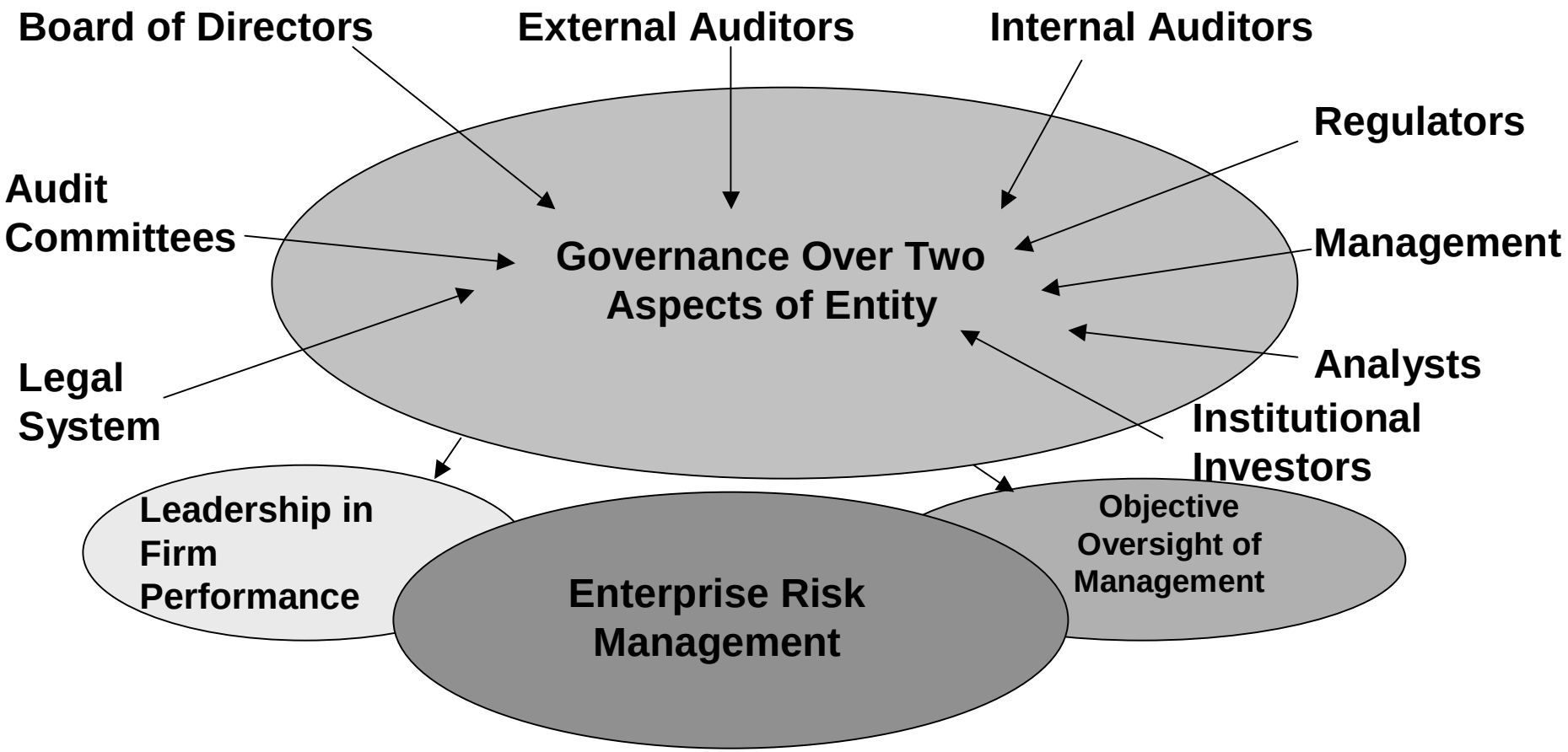
COSO's Definition of Risk

Risk is the possibility that an event will occur and adversely affect the achievement of objectives.

Characteristics:

- Present due to uncertainties
- All entities face risks
- Some risks can be opportunities
- Risks can erode or enhance value
- Risks arise from "internal" and "external" environment
- Risks evolve

How ERM Fits in Corporate Governance



COLLEGE OF MANAGEMENT
NC STATE UNIVERSITY

Upcoming Enterprise Risk Management Roundtables

"Launching ERM: Experiences from Progress Energy"

April 16, 2004

"Leveraging Sarbanes-Oxley to Create an ERM Process: Blue Cross Blue Shield's Experience

May 21, 2004