



Enterprise Risk Management

CFO, Investments & Operational Risk Conference and Expo
June 4, 2007

What is “Enterprise Risk Management”?

- “Enterprise risk management (ERM) is a process, effected by an entity’s board of directors, management and other personnel, applied in a 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.”

The Committee of Sponsoring Organizations (COSO) of the
Treadway Commission,

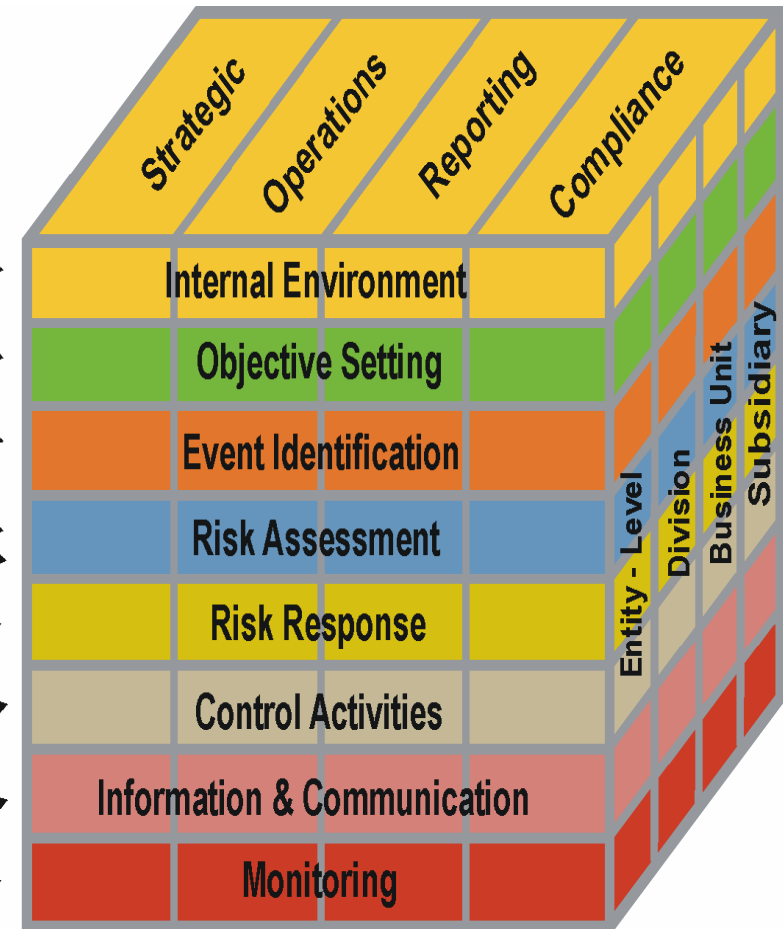
Enterprise Risk Management – Integrated Framework, September 2004

What is COSO?

- The COSO framework is a risk management tool that provides a big picture overview of the risks and related control environment.
- A direct relationship exists between a company's objectives and its processes, operations, and compliance, as management strives to achieve its objectives.

COSO's enterprise risk management framework

- What are we trying to accomplish?
- What could stop us from accomplishing it?
 - How bad are those scenarios?
 - Will they really happen?
- What are our options to stop those things from happening?
- How do we make sure they don't happen?
- How will we know that we've achieved what we wanted to accomplish?



Enterprise Risk Management (ERM)

- “What is being done to manage risks towards your strategic goals? Your operational goals? Or, your compliance and financial-reporting goals?”
- “Are risks that could affect the achievement of these goals identified and prioritized? Are you focusing on the right risks? How do you weigh them all against each other?”
- “Is your organization *too* risk averse?”

ERM | Continued

- All entities face uncertainty as they strive to achieve their strategic, operational, reporting and compliance goals.
- The challenge for management is to determine how much uncertainty to accept as it grows stakeholder value.

ERM | Continued

- Align risk appetite and strategy
- Enhance risk response decisions
- Reduce operational surprises and losses
- Identify and manage multiple and cross-enterprise risks
- Seize opportunities
- Improve deployment of capital

ERM | Continued

- The capabilities inherent in enterprise risk management help management achieve your performance and profitability targets and prevent loss of resources.
- ERM also helps ensure effective reporting and compliance with laws and regulations, and avoids damage to your reputation and the associated consequences.
- Finally, ERM helps you get to where you want to go, and avoid the pitfalls and surprises along the way

Risk Assessment Factors to Consider

- External/market reputation
- Financial
- Operational
- Legal/regulatory compliance
- Strategic
- Technology/systems
- People/culture
- Fraud

External / Market Reputation

- Defined as the risk that the business is exposed to losses in market value and value of company assets.
 - Significant interest rate fluctuation
 - Current volatility
 - Significant equity fluctuations

External / Market Reputation | Continued

- Competitor actions
- Credit worthiness
- Market/liquidity

Financial

- Defined as the risk that the organization's financial reporting is inaccurate, incomplete or untimely due to a variety of factors.
 - Achieving financial goals
 - Materiality
 - Volatility
 - Use of significant estimates

Operational

- Defined as the risk that the organization does not provide timely, accurate, authorized and complete processing activities to support the service or products to customers.
 - Inefficient/ineffective process design
 - Inadequate delivery of outsourced activities
 - Insufficient customer suitability assessment

Operational | Continued

- Employee error
- Inappropriate data usage
- Non-routine/complex transactions
- Compliance with policies and procedures
- Business interruption

Legal / Regulatory

- Defined as the risk that the organization fails to comply with a variety of federal, state and local laws, regulations and directives.
 - Legal and economic impact
 - Unresponsive to legal/regulatory/compliance change
 - Litigation issues
 - Highly regulated industry
 - Major consumer compliance regulations

Strategic

- Defined as the risk that business objectives will not be achieved because business strategies are poorly defined, communicated or the organization is unable to execute these strategies.
 - Insufficient or inadequate strategic planning
 - Ineffective organizational structure and alignment

Strategic | Continued

- Integration/alignment of IT infrastructure
- People or key resources
- Organizational reputation

Technology / Systems

- Defined as the risk of level of use, sophistication, complexity, etc. of systems within the organization.
 - Lack of information integrity
 - Inappropriate infrastructure
 - Lack of timely, reliable and relevant decision-making

Technology / Systems | Continued

- Inadequate data security and access
- Unavailability and instability of systems
- Sensitivity of data

People / Culture | Continued

- Defined as the risk of influence of cultural factors in the organization such as ethical tone, type of behavior encouraged and consistency of enforcement.
 - Inability to attract, train and retain intellectual capacity
 - Lack of clear roles and responsibilities
 - Deficient values, integrity and ethics
 - Inappropriate performance incentives

Fraud

- Defined as the risk of the structure of business activities and transaction processing and the business units susceptibility to both internal and external fraud.
 - Fraudulent financial reporting
 - Misappropriation of assets
 - Expenditure and liabilities for improper assets

Fraud | Continued

- Fraudulently obtained revenue and assets, and costs and expenses avoided
- Internal fraud
- Misconduct/abuse
- External crime
- External fraud

Benefits of ERM

- Enterprise-wide management of risk
- Management of risks to strategic, operational, compliance and reporting goals
- Effective internal controls to help address risk before it begins
- Aligning risk appetite and strategy

Benefits of ERM | Continued

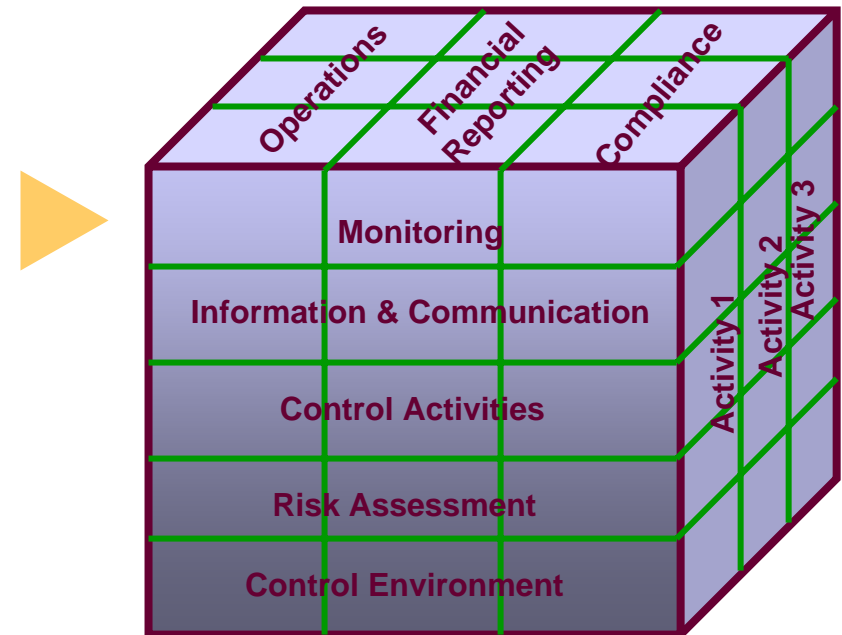
- Enhancing risk response decisions; reducing operational surprises and losses
- Identifying and managing multiple and cross-enterprise risks
- Seizing opportunities
- Improving deployment of capital

COSO Based Methodology

Monitoring

- Supervisory and managerial reviews
- Internal and external audit
- Management and Board oversight
- Independent evaluation

The COSO Model

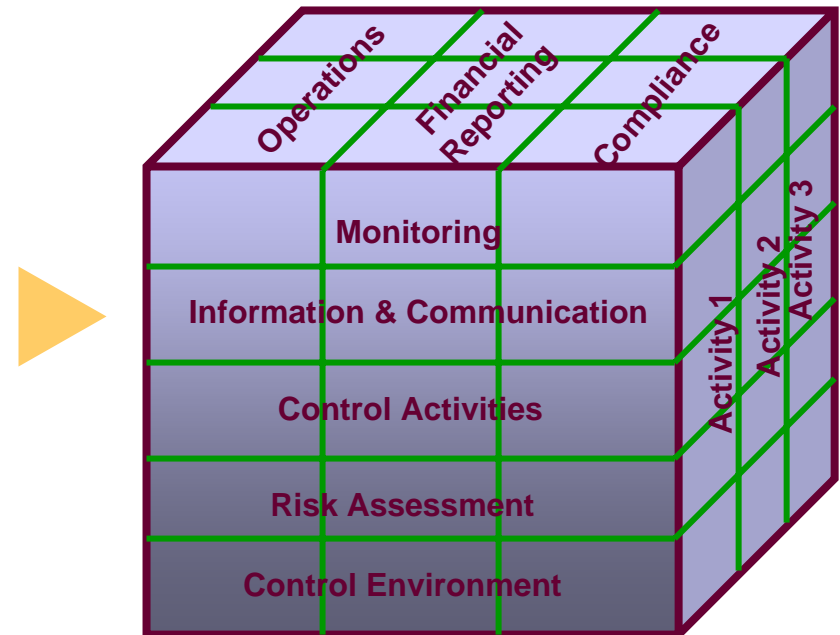


COSO Based Methodology | Continued

Information and Communication

- Internal management reports
- Business decision making
- External information analyzed
- Organization communication programs

The COSO Model

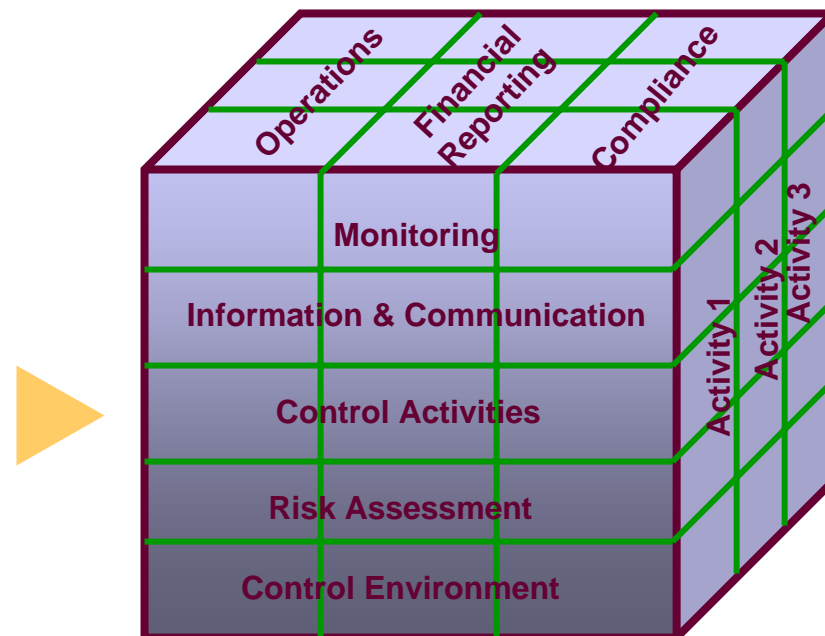


COSO Based Methodology | Continued

Control Activities

- Approvals and authorizations
- Policies and procedures
- Verification and reconciliation
- Segregation of duties

The COSO Model

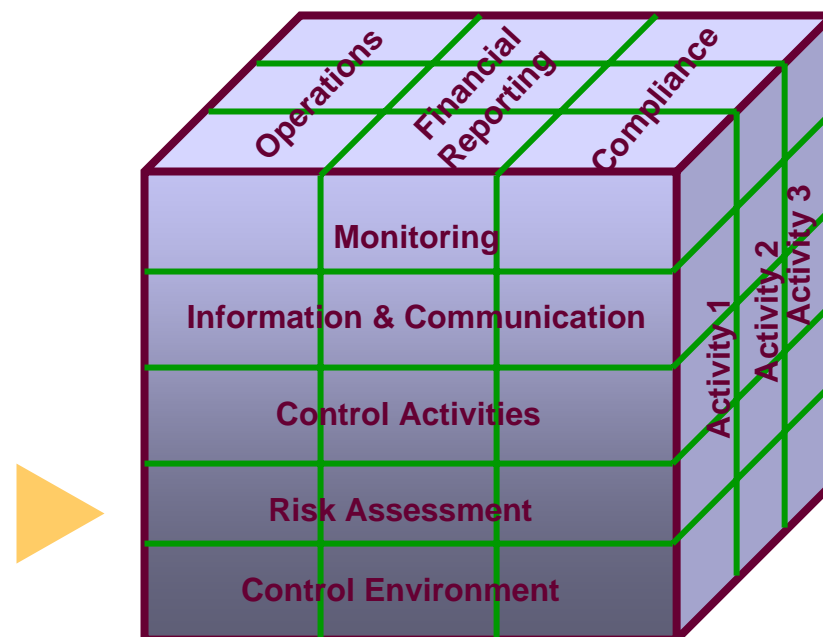


COSO Based Methodology | Continued

Risk Assessment

- Management's objectives
- Identification of risk
- Analysis of risk
- Management of risk
- Management of change

The COSO Model

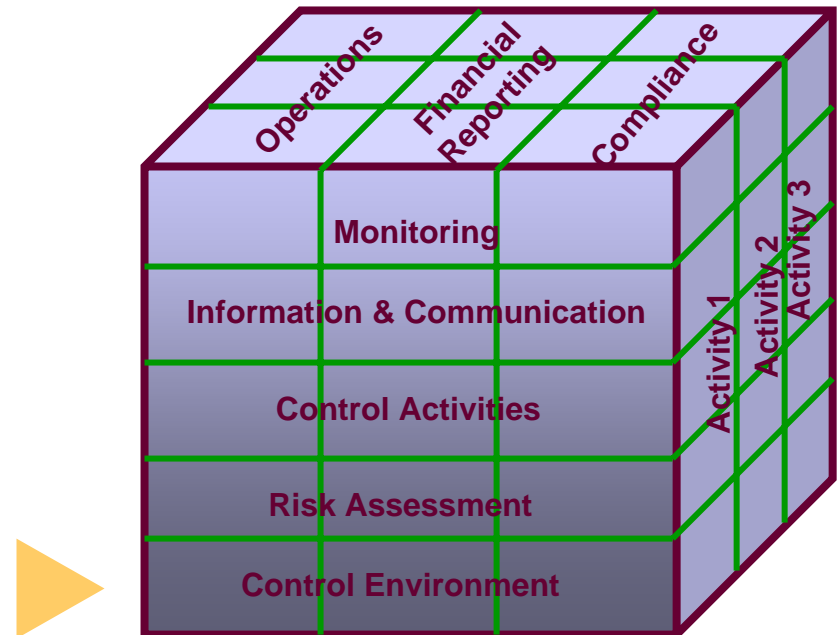


COSO Based Methodology | Continued

Control Environment

- Control is everyone's job
- Integrity and ethical values
- Management philosophy
- Authority and responsibility
- Human resource policies

The COSO Model



Risk Assessment Report

Business Area	Information	Financial Management	Legal/Regulatory	Safeguard of Assets	Operational	Technology	Strategic/Management	Risk Score
Lines of Business								
▪ Asset and Liability Management/ Investments	High	High	Low	High	Mod	Low	Low	213
▪ Personal Trust	Mod	Low	High	High	Mod	High	Low	213
▪ Retail Branch Activities	Low	Low	High	Low	High	Low	Mod	163
▪ Accounting	High	Mod	Mod	Low	Low	Low	Low	166
▪ Credit Underwriting	High	High	Mod	High	High	Low	High	261
▪ Deposit Operations	Low	Low	Mod	Mod	Mod	Low	Low	141
▪ Electronic Banking	Low	Low	Mod	Low	Mod	Mod	Mod	150
▪ Human Resources	Mod	Low	High	Low	Mod	Low	Low	157
▪ Loan Operations	High	Low	High	Mod	Mod	Low	Low	190
▪ Proof and Transit	Mod	Low	Low	Mod	Low	High	Low	159
▪ Wire Transfer and ACH	Mod	Low	High	High	Mod	Low	Low	186