



PRESENTATION  
ON  
ENTERPRISE RISK  
MANAGEMENT

---

AT WIRC, ICAI - MUMBAI  
8-8-2015

By CA AMIT PANDIT

# Defining risk...

A [probability](#) or [threat](#) of [damage](#), [injury](#), [liability](#), [loss](#), or any other negative occurrence that is caused by external or internal [vulnerabilities](#), and that may be avoided through preemptive [action](#).

- [www.businessdictionary.com](http://www.businessdictionary.com)

The chance that an [investment](#)'s actual [return](#) will be different than expected. Risk includes the possibility of losing some or all of the original investment. Different versions of risk are usually measured by calculating the [standard deviation](#) of the [historical returns](#) or [average returns](#) of a specific investment. A high standard deviation indicates a high degree of risk.

-[www.investopedia.com](http://www.investopedia.com)

## Defining risk...

*“A risk is a situation that an event, action, or non-action could adversely affect an organization’s ability to achieve its business objectives.”*

# Risk is Deviation from what is expected / budgeted



# How Do You See Risk

- You are given a bet
- Toss a coin
- Heads you get Rs 50 lakhs
- Tails you have to pay Rs 50 lakhs
- Will you take the bet?



## Definition of ERM

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

Source: COSO Enterprise Risk Management – Integrated Framework. 2004.  
The Committee of Sponsoring Organizations of the Treadway Commission (COSO)

# ERM Roles & Responsibilities

- Management
- The Board of Directors
- Top Management (CXOs, HODs etc)
- Internal auditors

# Evolution of Risk Management

- Safety and hazard management
- Process controls – Quality Controls
- Operations Risk Management
- Financial Risk Management
- Enterprise Risk Management – Integrated Framework



# Evolution of Risk Management

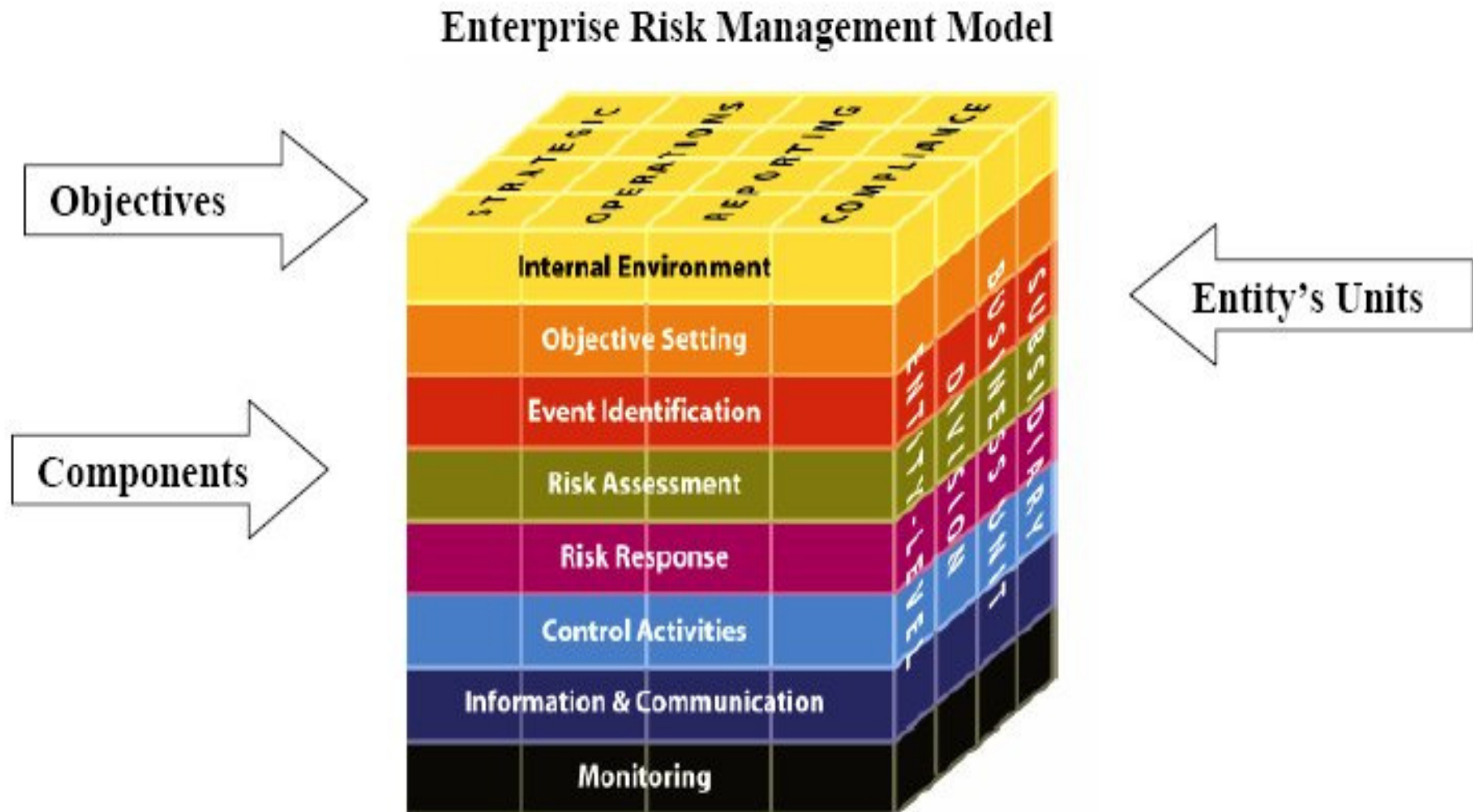


# Evolution of Risk Management – The Juggling Act Just Got Tougher

- Regulation
- Globalization
- Multi-Location operations
- Currencies – fx rates
- Interest rates
- Financial markets
- E-commerce



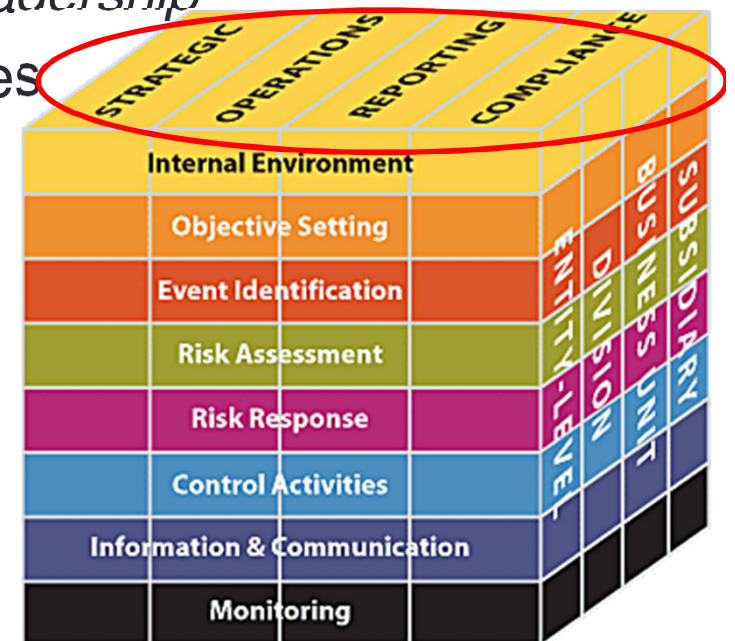
## ERM Model (As given by COSO)



# The ERM Framework

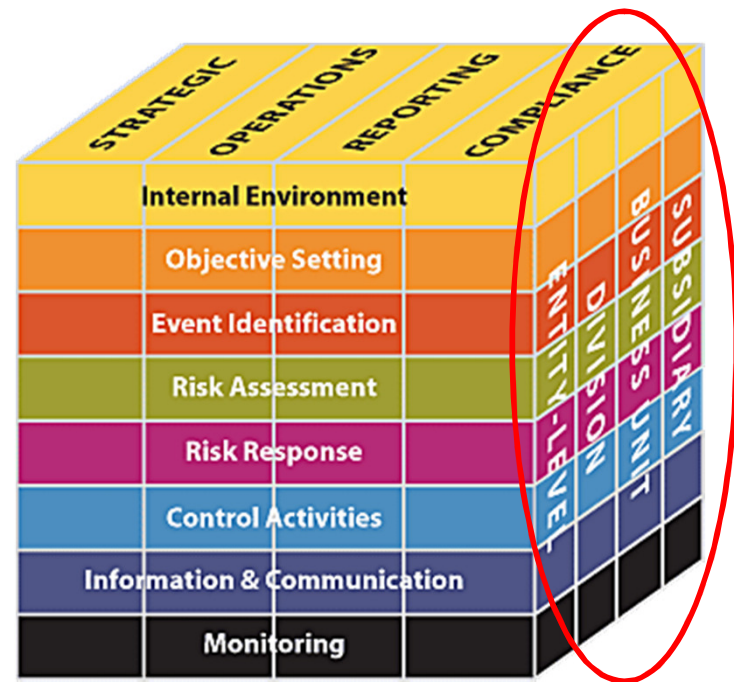
Objectives- Linked with Business Strategy Objectives

- Strategic- High level goals
  - *Eg. Attaining market share, Maintaining Leadership*
- Operations – Efficient use of Resources
  - *Eg Zero defect policy, Product Quality, Customer Service etc*
- Reporting
  - *Reliability with Financial Reporting, Clause 49, IFC*
- Compliance
  - *With All applicable Laws etc*



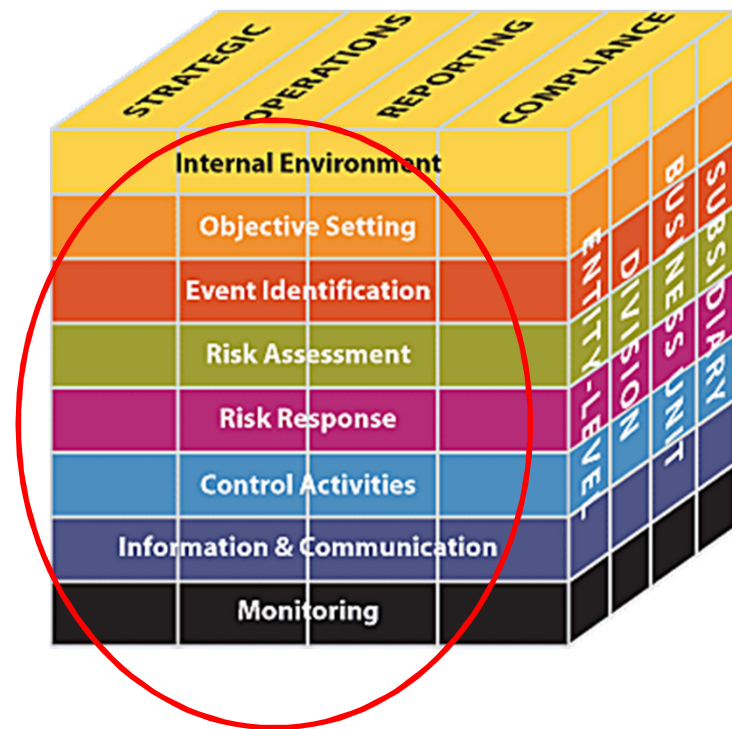
# The ERM Framework

- Develop a portfolio view
  - Entity level
  - Business unit level
  - Subsidiary/Division



# The ERM Framework

All Components are  
Interrelated



# Internal Environment

- Tone at the Top- Board
- Control Framework
- Establishes the entity's risk culture.
- Risk Philosophy & Risk Appetite
- Integrity & Ethical values
- Commitment to Compliance
- Considers all other aspects of how the organization's actions may affect its risk culture.
- Egs: Enron, Worldcom, Satyam
- Egs: Infosys, Walt Disney



# Objective Setting

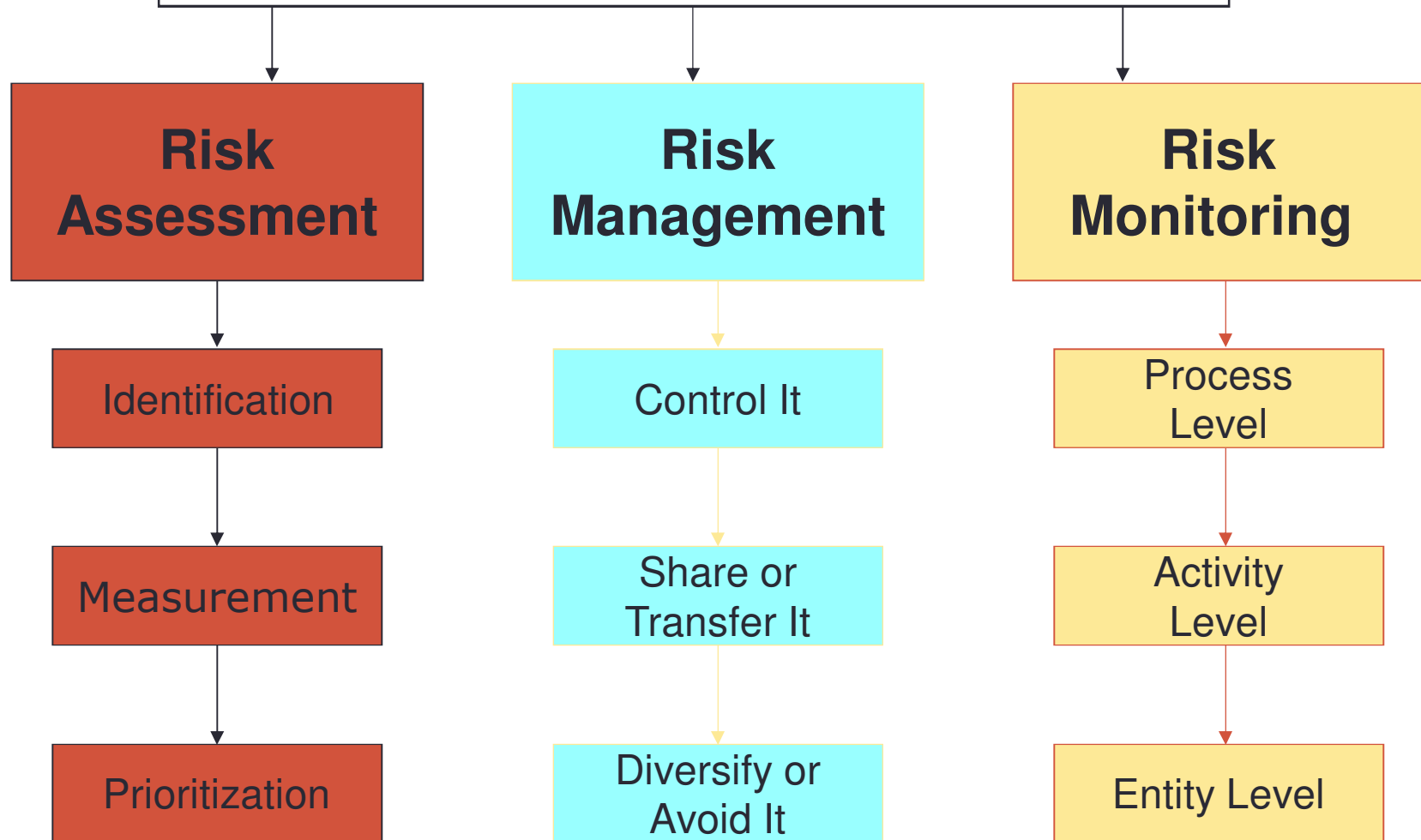
- Strategic Planning- How does business achieve its objectives
- Define risk appetite.
- Risk tolerance.
- Costs Involved
- Assignment of responsibilities to organizational elements and leaders (linkage)



# Event Identification

- Events that impact achievement of Objectives
  - Identify external & Internal Events.
  - Economic Events
  - Natural Disasters
  - Political Events
  - Technological Changes
  - Personnel Issues
  - Process Deficiencies
- Distinguish Risks and Opportunities.
- Understand how these events would influence the company risk.
- Identify List of Potential Risks
- Sit with each HOD to list things which can go wrong

# Risk Analysis



# Risk Assessment

- Assess risks from
  - Likelihood (Probability of Occurrence)
  - Impact
- Risk assessment methodologies.
- Assess risk (Inherent & Residual) .

## Likelihood Of Risk

<b>Level</b>	<b>Likelihood Definition</b>
<b>Certain</b> >90%	There is Certainty that Risk will occur
<b>Likely</b> 65-90%	It is Highly likely that Risk will occur
<b>Moderate</b> 35-65%	Possible Chance that Risk may occur
<b>Unlikely</b> 10-35%	It is Unlikely that Risk may occur
<b>Rare</b> <10%	There is an extremely remote chance that Risk may occur

<b>Magnitude of Impact</b>	<b>Risk Level Definition</b>
<b>Critical/ Extreme</b>	<b>Risk is catastrophic enough to impact business survival and an immediate intervention is required.</b>
<b>Major</b>	<b>High risk exists; action plans must be developed and reviewed frequently. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.</b>
<b>Moderate</b>	<b>Corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.</b>
<b>Minor</b>	<b>The risk is very low in significance or impact is minor which the organisation can decide to accept the risk.</b>
<b>Trivial</b>	<b>The impact is insignificant. No action required</b>

# Risks Matrix

*Risk Score = Probability of Occurrence (Likelihood) x Value of Impact*

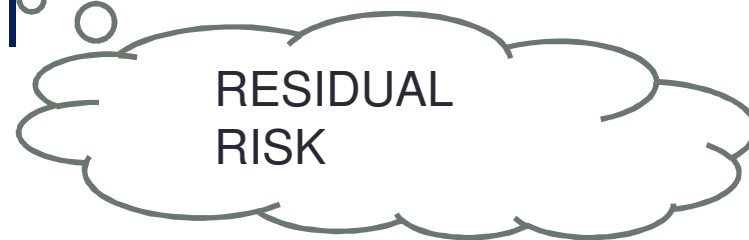
<b>Value of Impact</b>	<b>Critical (5)</b>	Treatable Risk (5)	<b>Treatable Risk (10)</b>	<b>Significant Risk (15)</b>	Significant Risk (20)	Significant Risk (25)
	<b>Major (4)</b>	Acceptable Risk (4)	Treatable Risk (8)	<b>Treatable Risk (12)</b>	Significant Risk (16)	Significant Risk (20)
	<b>Moderate (3)</b>	Acceptable Risk (3)	Treatable Risk (6)	Treatable Risk (9)	<b>Treatable Risk (12)</b>	<b>Significant Risk (15)</b>
	<b>Minor (2)</b>	Acceptable Risk (2)	Acceptable Risk (4)	Treatable Risk (6)	Treatable Risk (8)	<b>Treatable Risk (10)</b>
	<b>Trivial (1)</b>	Acceptable Risk (1)	Acceptable Risk (2)	Acceptable Risk (3)	Acceptable Risk (4)	Treatable Risk (5)
		<b>Rare (1)</b>	<b>Unlikely (2)</b>	<b>Moderate(3)</b>	<b>Likely (4)</b>	<b>Certain (5)</b>
<i>Probability of Occurrence</i>						

# Risk Response

- Evaluate Response options
- Risk Avoidance
- Risk Treatment (eg improving the internal control system)
- Risk transfer (Buying insurance)
- Risk Acceptance- (Monitoring)
- Risk Exploitation take advantage of the opportunities presented
- Residual Risk- Unmitigated Part of Risk

# Control Activities

- Preventive
- Detective
- Manual
- Automated
- Entity Level
- Process Level
- Application Level<sup>o</sup>





# Information & Communication

- Dashboard of risks and related responses (visual status of where key risks stand relative to risk tolerances)
- Flowcharts of processes with key controls noted
- Narratives of business objectives linked to operational risks and responses
- List of key risks to be monitored or used
- Management understanding of key business risk responsibility and communication of assignments

# Monitoring

- Collect and display information
- Perform analysis
  - Risks are being properly addressed
  - Controls are working to mitigate risks



# Internal Control

A strong system of internal control is essential to effective enterprise risk management.

# Internal Auditors

- Do not have primary responsibility for ERM implementation or maintenance.
- Can Assist management in the process by:
  - Monitoring
  - Evaluating
  - Examining
  - Reporting
  - Recommending improvements



Email: [pandit.amit.ca@gmail.com](mailto:pandit.amit.ca@gmail.com)

Hand Phone: +919820127898