

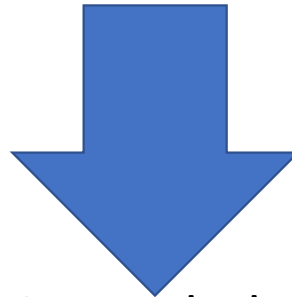


Internal Audit (ACCT 337)

Chapter 4 Enterprise Risk Management (ERM)

Definition of Risk

- *According to COSO*: The possibility that an event will occur and adversely affect the entity ability to achieve its objectives.
- BUSINESS OBJECTIVES  BUSINESS RISKS
- Single Objective  Multiple Risks



ERM is needed to:

1. understand
2. Assess
3. manage risks across the organization

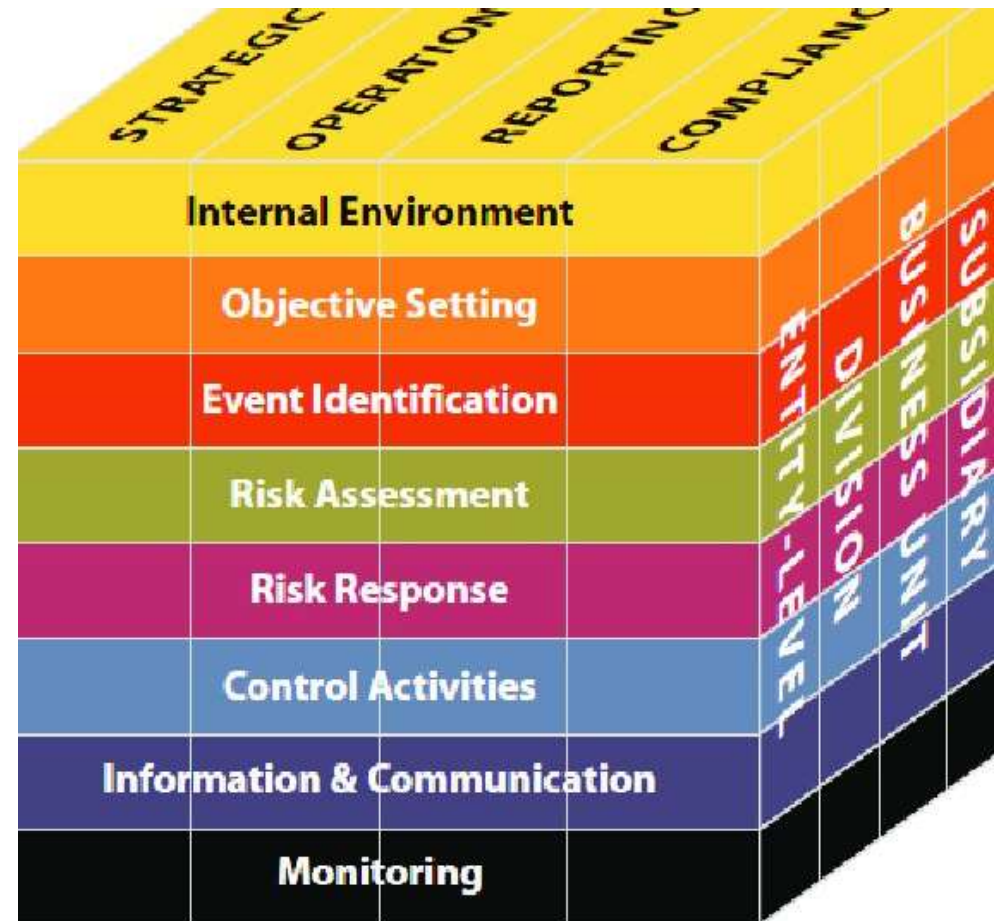
COSO ERM Framework

- Published in 2004 by COSO
- Expanded on COSO 1 (Internal Controls –Integrated Framework)
- **Enterprise risk management** 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 the entity objectives.

COSO ERM CUBE

3D Matrix:

1. Types of Objectives: 4 types
2. ERM Components: 8 *Interrelated components*
3. Organization Business Structure



ERM Components

C1- Internal Environment

- Foundation for all other components
- Include:
 - Risk management philosophy
 - Risk appetite
 - BOD
 - Integrity and ethical values
 - Organization structure
 - Assignment of authority and responsibility
 - HR policies and procedures

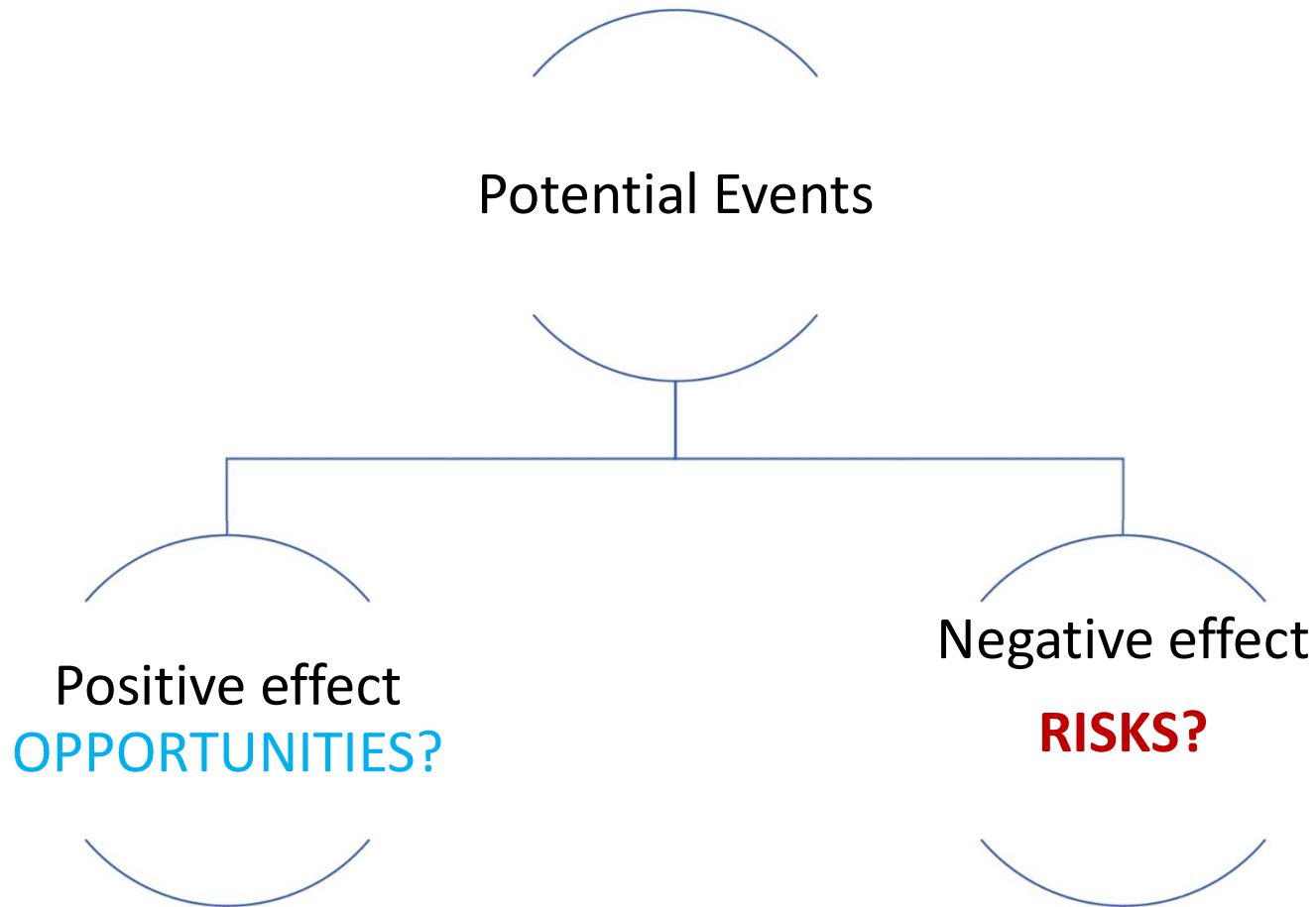
ERM Components

C2- Objective Setting

- Four types of objectives
- Precondition?

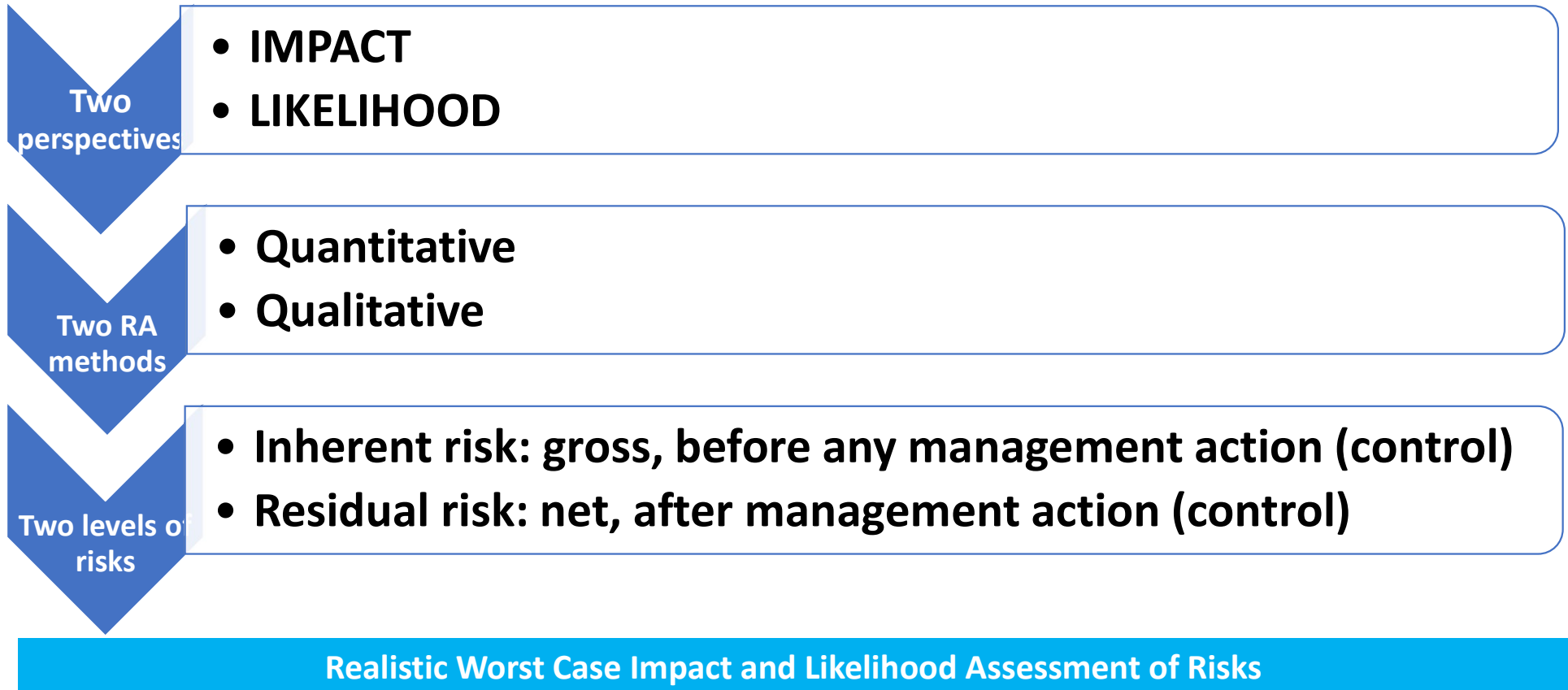
ERM Components

C3- Event Identification



ERM Components

C4- Risk Assessment



ERM Components

C5- Risk Response

- Factors to consider:
 - Risk Rating
 - Cost and benefit
 - Risk residual and risk tolerance
- Four Types (Strategies) of Risk Responses
 1. Avoidance?
 2. Reduction?
 3. Sharing?
 4. Acceptance?

ERM Components

C6- Control Activities

Ps & PS to help ensure that risk Responses are carried out.

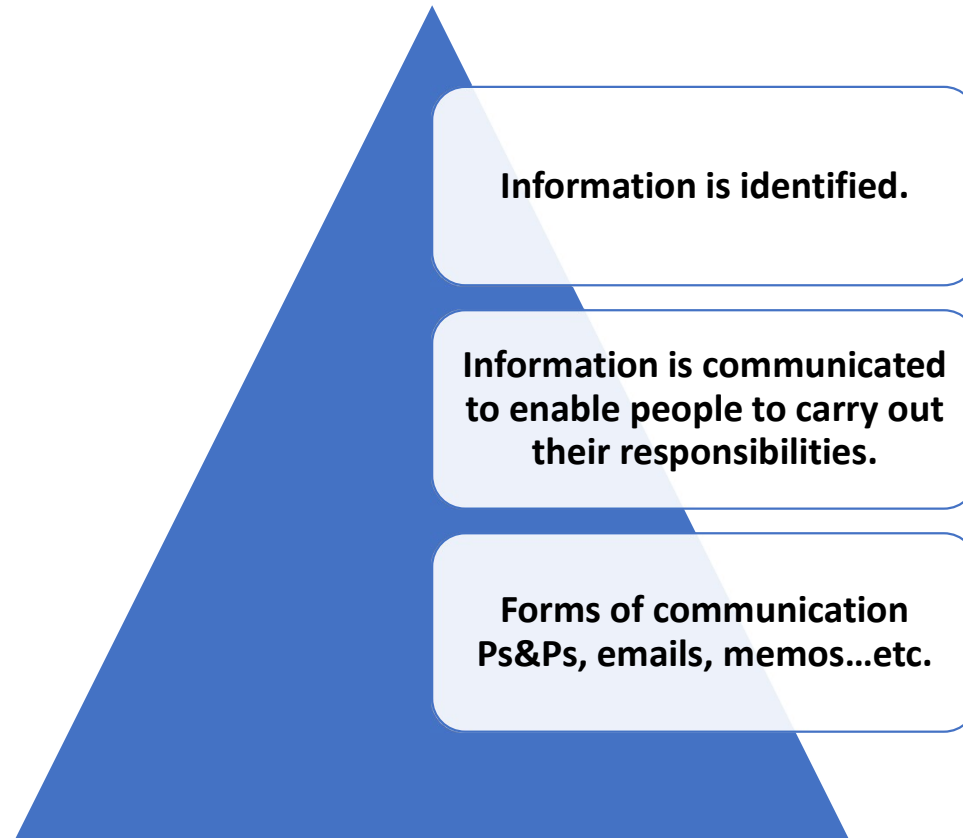
Risk Reduction Strategy.

Examples:

- Top Level Reviews
- Direct Functional or Activity Management Review
- Physical Controls
- SOD : A/R/C/R

ERM Components

C7- Information and Communication



ERM Components

C8- Monitoring

To assess the existence and functioning of all other ERM components over time.



Two methods

- Self Assessment
- Separate Evaluations: IA, External Auditor

Chief Risk Officer (CRO)

Senior management
position

Focal point to
facilitate RM activities

Risk Management
and Compliance
Fuction

ERM Responsibilities

BOD?

Management?

Internal Auditor?

End of Chapter