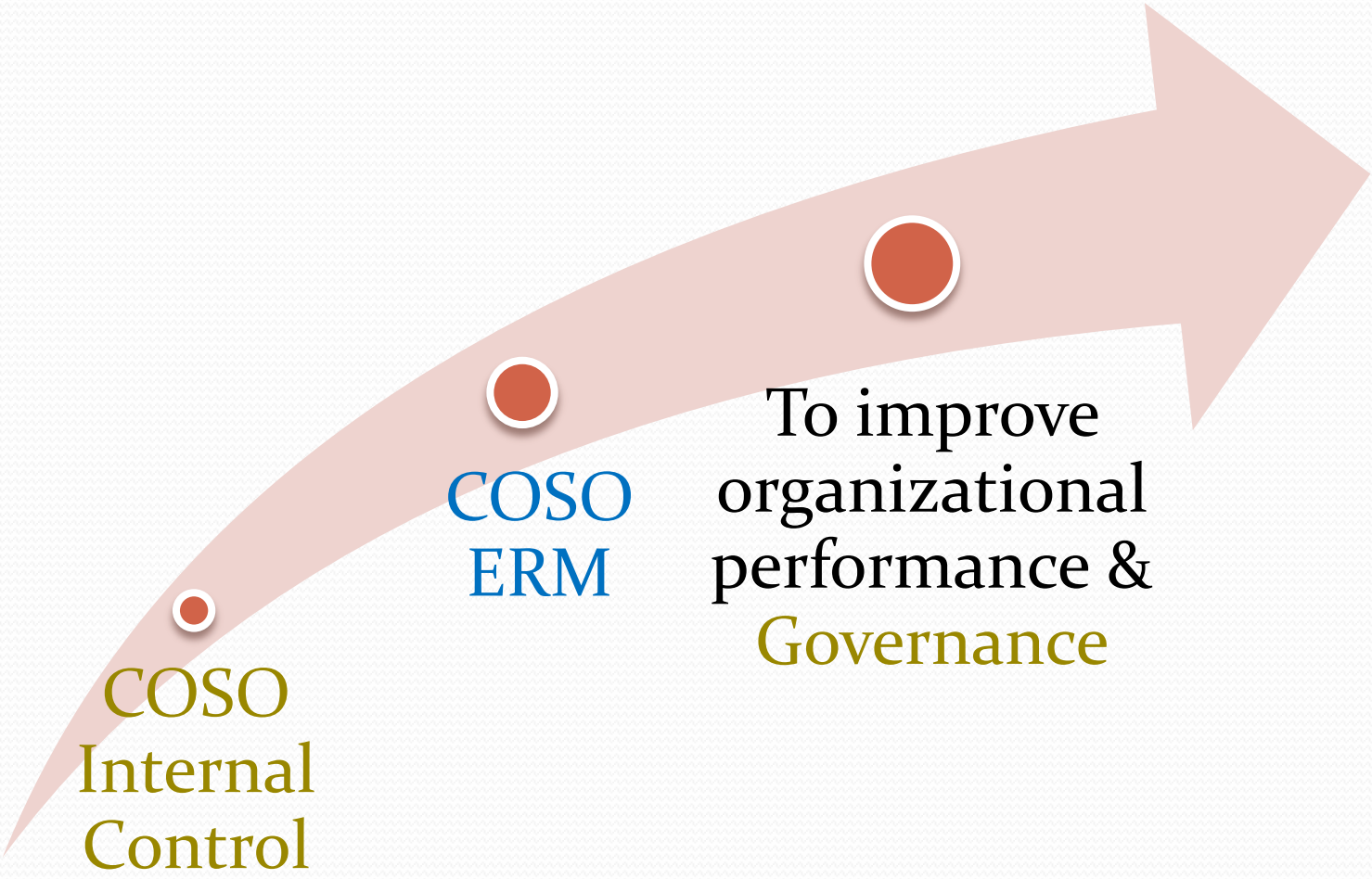
COSO Enterprise Risk Management (ERM)

COSO ERM


COSO Internal Control
COSO ERM
To improve organizational performance & Governance

COSO ERM

- Definition of Enterprise Risk Management (ERM)

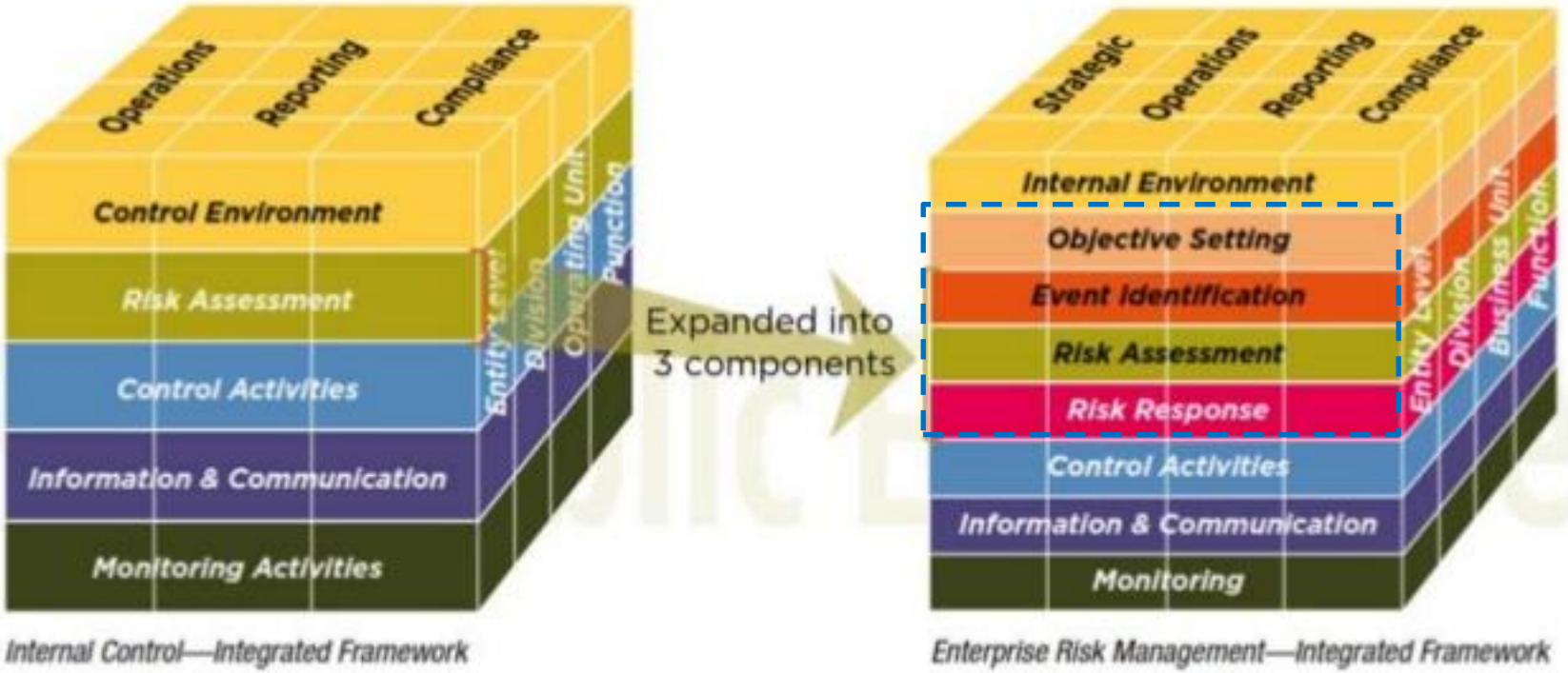
  → A process applied in strategy-setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives

From COSO to COSO ERM

- Additional components
  - (Strategic) Objective Setting (2nd)
  - Event Identification (3rd)
  - Risk Response (5th)

Note: Risk Assessment →
- Event Identification
- Risk Assessment
- Risk Response

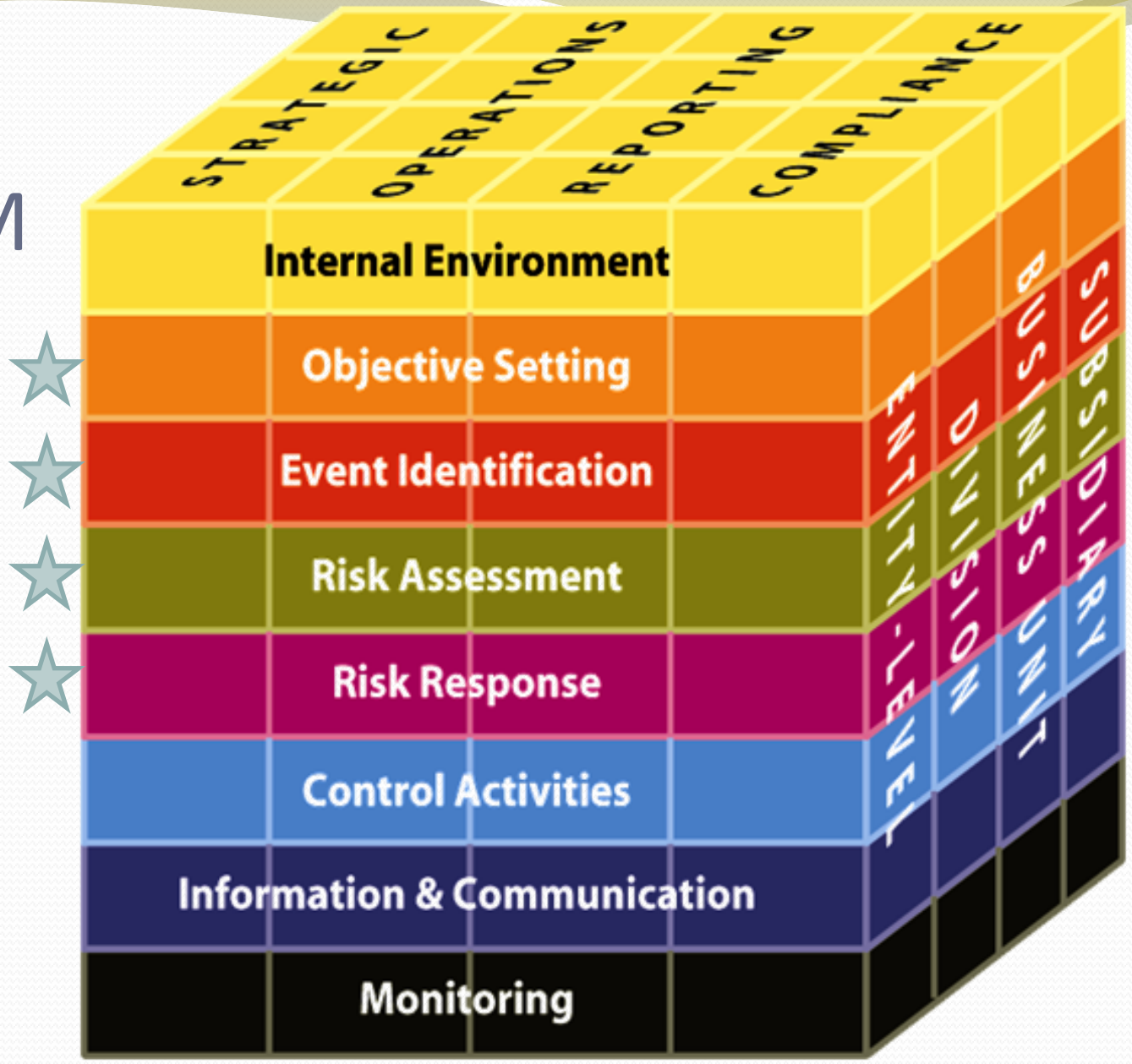
COSO IC vs. COSO ERM



Internal Control—Integrated Framework

Enterprise Risk Management—Integrated Framework

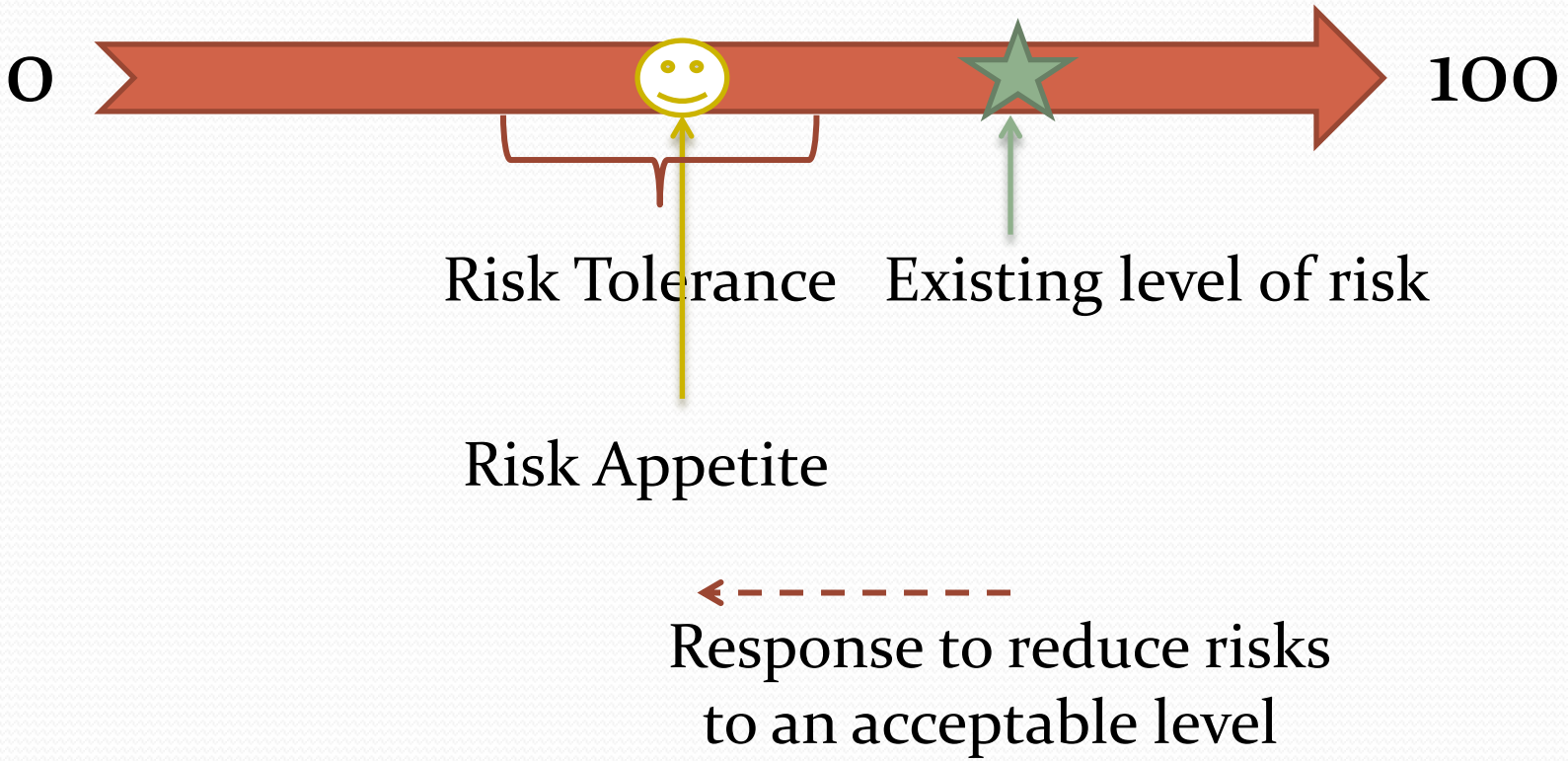
COSO ERM


STRATEGIC
OPERATIONS
REPORTING
COMPLIANCE
Internal Environment
Objective Setting
Event Identification
Risk Assessment
Risk Response
Control Activities
Information & Communication
Monitoring
ENTITY-LEVEL
DIVISION
BUSINESS UNIT
SUBSIDIARY

Objective Setting

- Strategic and related objectives are established.
  - Strategic objective
    → A high-level, broadly defined and externally focused objective that an organization must achieve to support its mission and to make its strategy succeed.
    Ex. Market share, Innovation or Social responsibility
- Risk Appetite and Risk Tolerances are considered.
  - Risk Appetite → The level of risk an organization is prepared to accept.
  - Risk Tolerance → Acceptable level of variation of risk an entity is willing to accept .

Risk Appetite & Risk Tolerance



Event Identification

- Consider a range of potential events from both internal and external sources without focusing on positive (opportunity) or negative (risk) impacts
  - Ex.

Potential Event	Opportunity	Risk
1. AEC (External)	Larger markets More customers	More competitors Language
2. New accounting software (Internal)	More efficient in processing accounting information	Lack of technical skill leading to unintentional mistakes

Event Identification (cont.)

External Events	Internal Events
✓ Economic factors → Unemployment, Competition ✓ Environmental factors → Natural disaster ✓ Political factors → Public policy, Government change ✓ Social factors → Demographics, Consumer behavior ✓ Technological factors → E-Commerce	✓ Infrastructure factors → Access to capital/fund ✓ Personnel factors → Competency, Fraud ✓ Process factors → Capacity, Supplier dependency ✓ Technological factors → System selection, Maintenance

Risk Assessment

- More elaborate than that in COSO Internal Control
- Consider "Inherent risk" and "Residual Risk"

Inherent risk → Response → Residual risk at an acceptable level

- Consider 1) Likelihood of occurrence
  2) Severity of Impact
  3) Velocity of Impact
  4) Persistence of Impact
  } Impact

  in order to analyze and prioritize risks

Risk Response

- Target: To select possible alternatives for reducing risk to an acceptable level
- Solutions:
  - Risk Avoidance → avoid to confront risks
  - Risk Acceptance → accept risk when it is at an acceptable level
  - Risk Sharing → Share risk to others (Insurance, Hedging, Outsourcing)
  - Risk Reduction → Reduce risk through internal control system

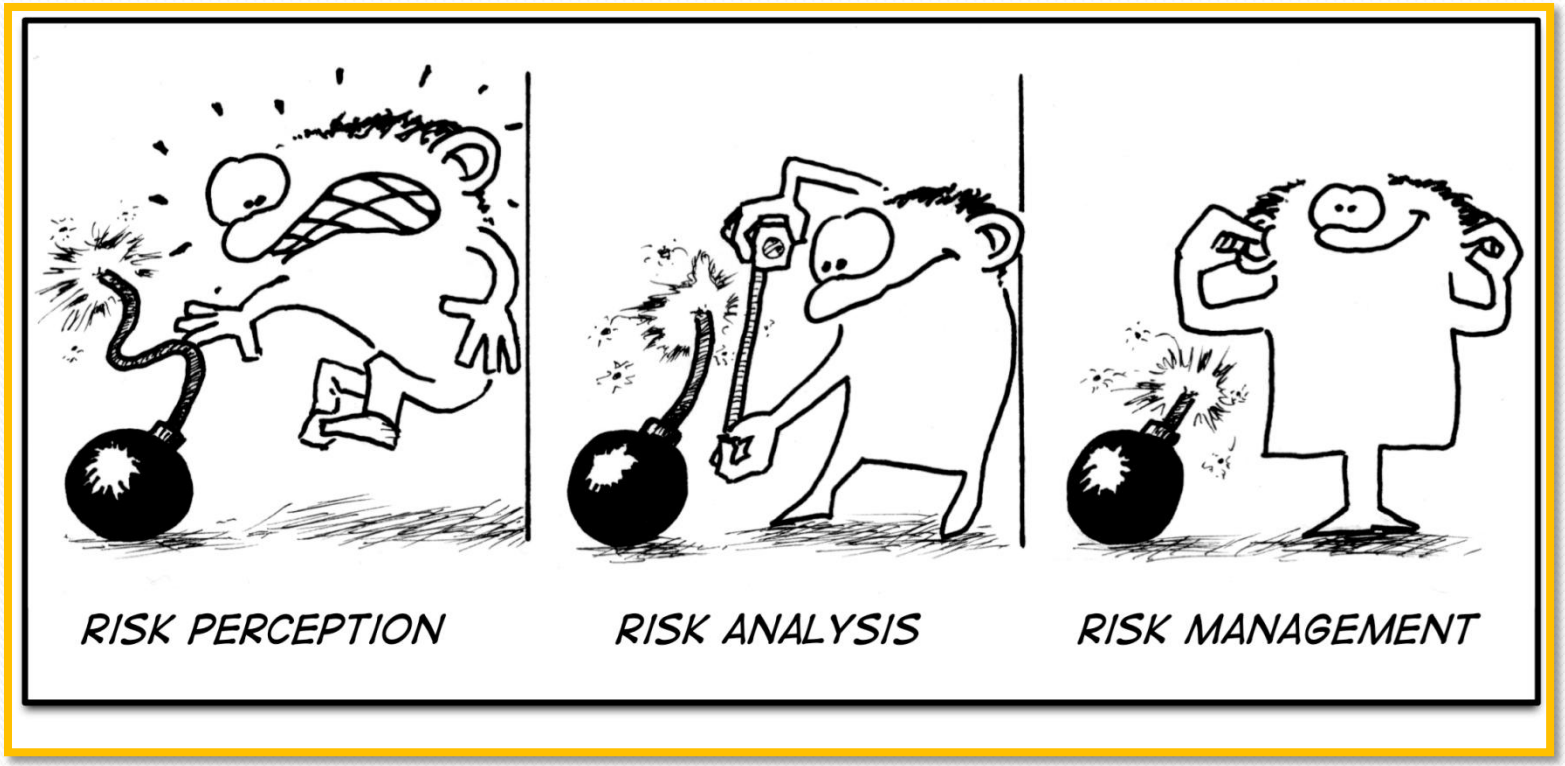
Limitations

- Human judgment in decision making can be faulty.
- Costs and benefits
- Human failures such as errors or mistakes
- Controls can be circumvented by collusion of two or more.
- Management has the ability to override enterprise risk management decisions.

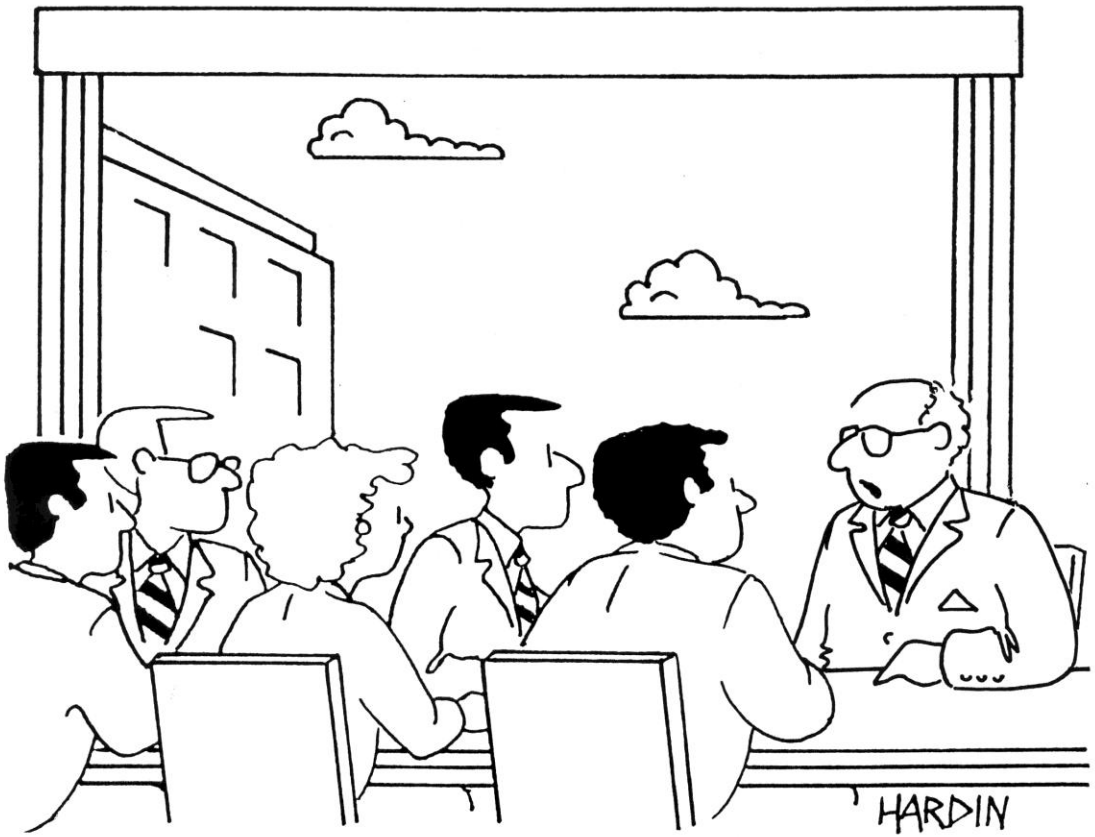
Summary: Differences

COSO Internal Control	COSO ERM
• Objectives: 1) Operations 2) Reporting 3) Compliance → focused only on "Internal factors"	• Adding "Strategic objective" which depends on "External factors"
• Risk response → mostly by trying to reduce risk (Risk Reduction)	• Risk response → 4 methods: 1) Risk Avoidance 2) Risk Acceptance 3) Risk Sharing 4) Risk Reduction

Just for fun



Just for fun


HARDIN
"We've considered every potential risk except the risks of avoiding all risks."