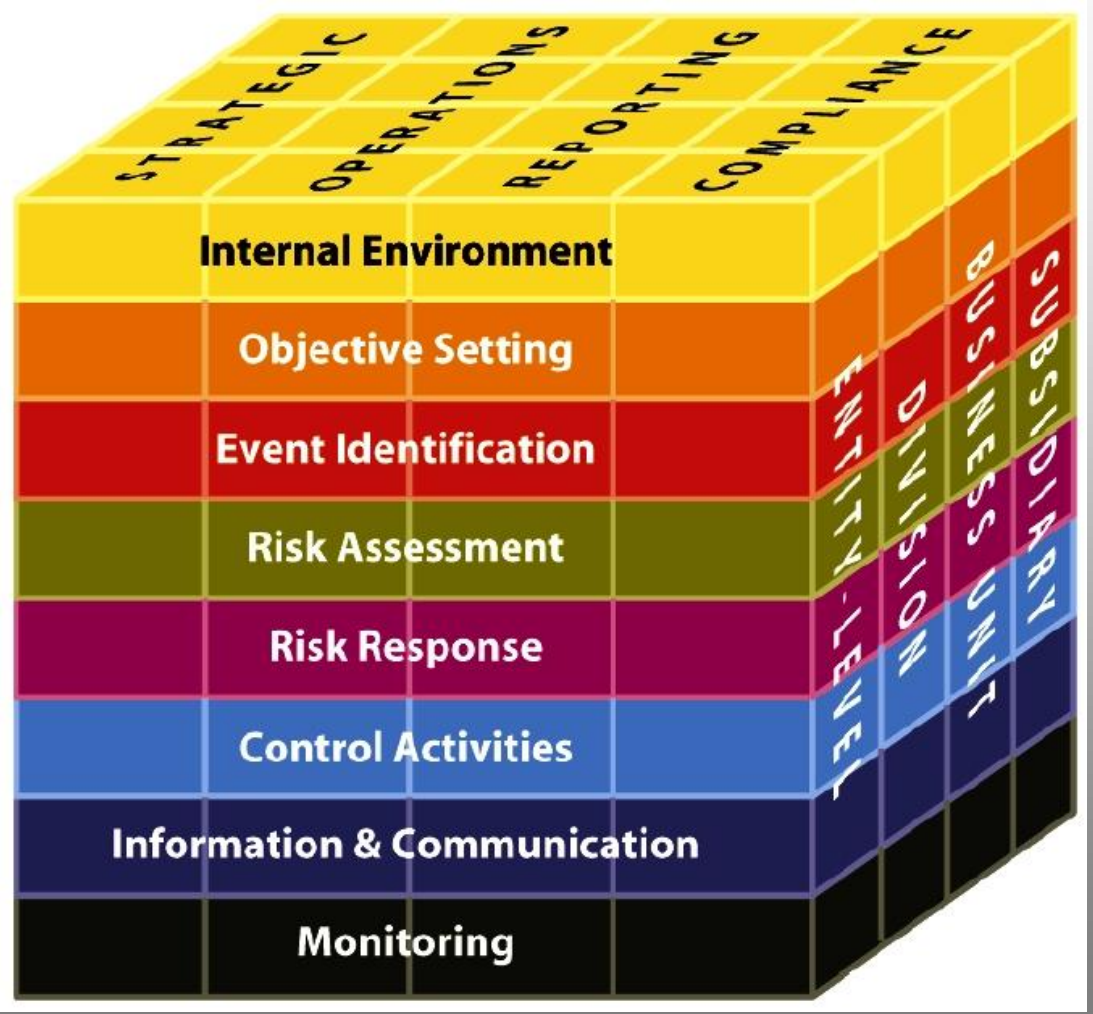
Enterprise Risk Management

Take a Close Look at COSO's New Internal Control Framework

Eight Components

Three more layers added to the original five COSO components:

- **Internal Environment**
- **Objective Setting**
- **Event Identification**



Four Objectives

Strategic objective added to the original three COSO objectives:

- **Operations**
- **Reporting***
- **Compliance**

* **Reporting is now much more than financial reporting**

Internal Environment

The internal environment encompasses the tone of an organization, influencing the risk consciousness of its people, and is the foundation for all other components of enterprise risk management, providing discipline and structure.

Internal environment factors include:

- an entity's risk management philosophy;
- its risk appetite and risk culture;
- oversight by the board of directors;
- the integrity, ethical values and competence of the entity's people;
- management's philosophy and operating style; and
- the way management assigns authority and responsibility, and organizes and develops its people.

Objective Setting

Every entity faces a variety of risks from external and internal sources, and a precondition to effective event identification, risk assessment and risk response is establishment of objectives, linked at different levels and internally consistent.

Objectives are set at the strategic level, establishing a basis for operations, reporting, and compliance objectives.

Objectives are aligned with the entity's risk appetite, which drives risk tolerance levels for the entity's activities.

Event Identification

Management identifies potential events affecting an entity's ability to successfully implement strategy and achieve objectives.

Events with a potentially negative impact represent risks, which require management's assessment and response.

Events with a potentially positive impact may offset negative impacts or represent opportunities. Management channels opportunities back into the strategy and objective-setting processes.

A variety of internal and external factors give rise to events. When identifying potential events, management considers the full scope of the organization. Management considers the context within which the entity operates and its risk tolerances.

Risk Assessment

Risk assessment allows an entity to consider the extent to which potential events might have an impact on achievement of objectives.

Management should assess events from two perspectives – likelihood and impact – and normally uses a combination of qualitative and quantitative methods.

The positive and negative impacts of potential events should be examined, individually or by category, across the entity.

Potentially negative events are assessed on both an inherent and a residual basis.

Risk Response

Having assessed relevant risks, management determines how it will respond.

Responses include risk avoidance, reduction, sharing and acceptance.

In considering its response, management considers costs and benefits, and selects a response that brings expected likelihood and impact within the desired risk tolerances.

Control Activities

Control activities are the policies and procedures that help ensure that management's risk responses are carried out.

Control activities occur throughout the organization, at all levels and in all functions.

They include a range of activities as diverse as:

- approvals,
- authorizations,
- verifications,
- reconciliations,
- reviews of operating performance,
- security of assets, and
- segregation of duties.

Information and Communication

Pertinent information is identified, captured and communicated in a form and timeframe that enable people to carry out their responsibilities. Information systems use internally generated data, and information about external events, activities and conditions, providing information for managing enterprise risks and making informed decisions relative to objectives. Effective communication also occurs, flowing down, across and up the organization. All personnel receive a clear message from top management that enterprise risk management responsibilities must be taken seriously. They understand their own role in enterprise risk management, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There is also effective communication with external parties.

Monitoring

Enterprise risk management is monitored –a process that assesses the presence and functioning of its components over time.

This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two. Ongoing monitoring occurs in the normal course of management activities.

The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures.

Enterprise risk management deficiencies are reported upstream, with serious matters reported to top management and the board.

Internal Environment

Risk Management Philosophy	Risk Appetite	Risk Culture	Board of Directors	Integrity and Ethical Values	Commitment to Competence
•Value •Communicate in words and actions	•Value •Qualitative •Quantitative •Linked to strategy	•Independent •Active •Involved	•Independent •Active •Involved	•Standards of behavior •Prerequisite •CEO example Incentives	•Knowledge •Skills •Trade-offs

Management Philosophy and Operating Style	Organizational Structure	Assignment of Authority and Responsibility	Human Resource Policies and Practices	Differences in Environment
•Formal vs. Informal •Conservative vs. Aggressive •Aligned	•Reporting lines •Centralized/ Decentralized •Matrix/Function/ Geography	•Empowerment •Accountability	•Qualified •Training •Compensation •Incentives and Discipline	•Management preferences •Value judgments •Management Styles

OBJECTIVE SETTING

Strategic Objectives	Related Objectives	Selected Objectives	Risk Appetite	Risk Tolerance
•High-level goals •Support mission/ vision •Strategic choices	•Operations •Reporting •Compliance •Safeguard-ing of assets	•Align and support •Manage-ment decision	•Growth, risk and return •Resource allocation •People, process and infrastructure	•Acceptable variance •Unit of measure of objective

EVENT IDENTIFICATION

Events	Factors Influencing Strategy and Objectives	Metho-dology and Techniques	Event Interdepen-dencies	Event Categories	Risks and Opportu-nities
•Incident •Positive and/ or negative impacts	•Internal •External	•Ongoing •Periodic •Past and future •Supporting tools	•Triggering events •Interrelate	•Common groupings	•Negative impact: risks •Positive impact: opportunity; offsets to risks

RISK ASSESSMENT

Inherent and Residual Risk	Likelihood and Impact	Qualitative and Quantitative Methodologies and Techniques	Correlation
•Before management actions •After management actions •Expected and unexpected	•Expected, worst-case, distribution •Time horizons •Unit of measure •Observable data	•Qualitative •Quantitative •Inherent and residual basis	•Sequence of events •Categories •Stress testing •Scenarios

RISK RESPONSE

Identify Risk Responses	Evaluate Possible Risk Responses	Select Response	Portfolio View
•Avoid •Reduce •Share •Accept	•Impact •Likelihood •Cost versus benefit •Innovative responses	•Management decision	•Entity level •Business unit level •Inherent and residual basis

CONTROL ACTIVITIES

Integration with Risk Response	Types of Control Activities	General Controls	Application Controls	Entity-Specific
•Build directly into management processes •Interrelate	•Policies •Procedures •Preventative •Detective •Manual •Automatic	•Information technology (IT) management •IT infra-structure •Security management •Software development & maintenance	•Completeness •Accuracy •Authorization •Validity	•Entity specific strategies and objectives •Operating environment •Complexity of the entity

INFORMATION & COMMUNICATION

Information	Strategic and Integrated Systems	Communication
•Internal •External •Manual •Computerized •Formal •Informal •Information systems architecture	•Strategic •Operational •Past and current •Level of detail •Timeliness •Quality	•Internal •External •Entity-wide •Expectations and responsibilities •Framing •Means of transmission

MONITORING

Ongoing	Separate Evaluations	Reporting Deficiencies
•Real-time •Built-in •Day-to-day operations	•Scope •Frequency •Self-assessments/ internal auditors •Extent of documentation	•Ongoing •External parties •Protocols •Alternative channels

For more information:

Check out COSO's exposure draft

Enterprise Risk Management Framework

At **www.erm.coso.org**

Download it in Adobe PDF format
(152 pages)