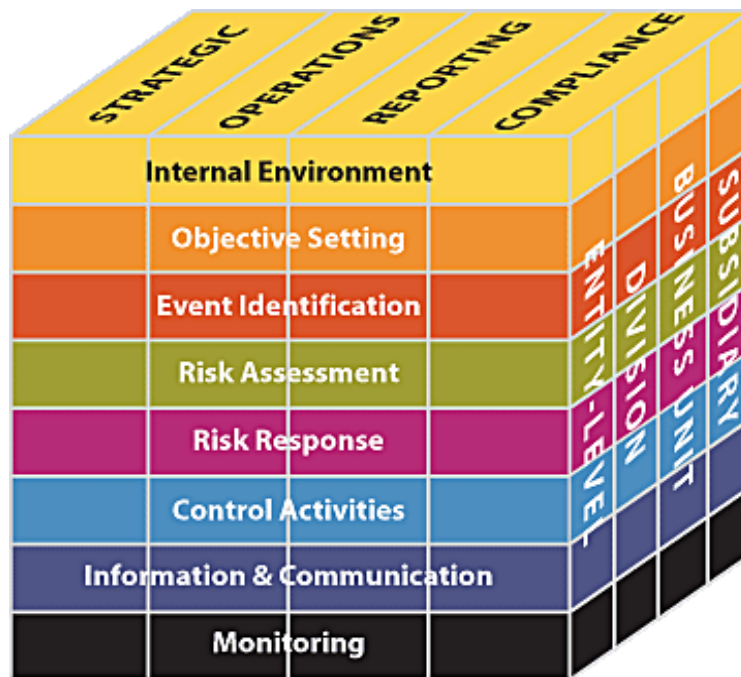# COSO Enterprise Risk Management Framework

COSO was first introduced in 1992 as an internal controls framework. It was subsequently supplemented in 2004 with the COSO ERM framework (above). The framework is one of the most comprehensive frameworks and is designed to offer organizations a widely accepted model for evaluating their risk management efforts. It is principles based which expands on internal control concepts by providing a more robust focus to ERM by recognizing that an effective ERM process must be applied within the context of strategy setting. It provides guidance to help organizations build effective programs for identifying, measuring, prioritizing and responding to risk.

In conjunction with the publication of COSO's "Enterprise Risk Management – Integrated Framework", a supplement was prepared providing guidance on application techniques. It provides examples to assist organizations with implementing an ERM program which can be used in whole or in part and modified to fit the organizations needs.

The COSO ERM framework has eight interrelated components.

- Internal Environment – refers to the tone of the organization, its risk appetite and elements such as board oversight.

- Objective Setting – refers to setting objectives at a strategic level, establishing a basis for operations, reporting and compliance objectives. Setting the objectives must be done before management can identify potential events affecting their achievement.

- Event Identification – management identifies potential events that could affect the entity either adversely or presents an opportunity and emanates from internal and external sources.

- Risk Assessment – consideration of the extent to which potential events have an impact on the achievement of the organizations objectives. Evaluate the risks that have been identified in order to form a basis for determining their management.

- Risk Response – after the determination of relevant risk, management determines how it will respond. This may include avoidance, reduction, sharing and acceptance.

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

- Information & Communication – refers to the proper information being identified, captured and communicated in an adequate format and timeframe to the appropriate individuals.

- Monitoring – assessing the functions and components of risk management over time and making adjustments as necessary.