Framework

The COSO Enterprise Risk Management—Integrated Framework is designed to help an organization achieve its objectives in four categories:

- Strategic—high-level goals, aligned with and supporting its mission
- Operations—effective and efficient use of its resources
- Reporting—reliability of reporting
- Compliance—compliance with applicable laws and regulations

There are eight interrelated components of the COSO framework that should be integrated within an organization's risk management process:

- Internal environment—Determine risk management philosophy and risk appetite, integrity and ethical values, and the operating environment. A board of directors is an important part of the internal environment with influence on the other aspects of the environment. In this component of the risk management process, senior management aligns the people, processes, and infrastructure to make it possible for the organization to stay within its risk appetite.
- Objective setting—Align risk management objectives with the organization's mission and risk appetite. Objectives must be determined before management can identify the events that might affect their achievement.
- Event identification—Identify internal and external events that affect achievement of objectives, and distinguish between negative risk and opportunity risk. External events include economic, political, social, and technological elements. Internal factors include management decisions, people, infrastructure, processes, and technology.
- Risk assessment—Analyze risks, considering likelihood and impact. Likelihood is the possibility that a given event will occur. Impact is the effect of an event if it does occur. Risk assessment is first applied to **inherent risk**. After the development of risk responses, **residual risk** is determined.
- Risk response—Select how to respond to the risks identified, for example, by avoidance, reduction, or transfer.
- Control activities—Establish policies and procedures to carry out effective risk responses. Control activities are the policies and procedures to determine that risk responses are performed correctly.
- Information and communication—Use effective communication that flows down, across, and up the organization. An organization should use both historical and current data to have an effective risk management program.
- Monitoring—Make modifications through ongoing monitoring of the risk management process. An organization may use both internal and independent evaluations to monitor its risk management.

Inherent risk

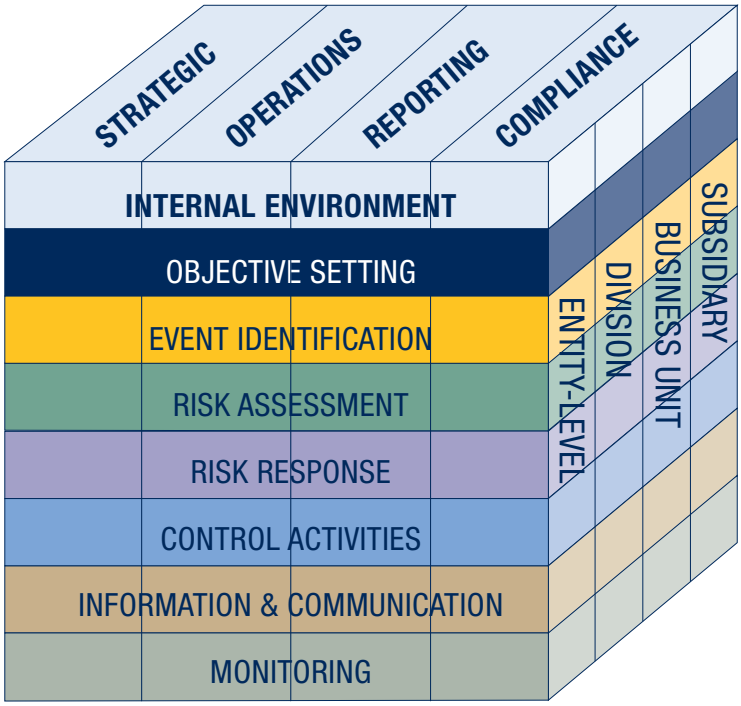
Risk to an entity apart from any action to alter either the likelihood or impact of the risk.

Residual risk

Risk remaining after actions to alter the risk's likelihood or impact.

COSO Risk Management: Relationship of Objectives and Components

There is a direct relationship between objectives, which an organization strives to achieve, and risk management components, which are necessary to achieve them.



COSO states that "risk management is not strictly a serial process, where one component affects only the next. It is a multidirectional…process in which almost any component can and does influence another."[11] The process should be applied across all four levels of an organization: entity, division, business unit, and subsidiary. See the exhibit "COSO Risk Management: Relationship of Objectives and Components."

In the example of a bank, the organization would identify its strategic objectives to include return on capital, profit, and growth. The bank's operational objectives would support its strategic objectives in areas such as loan activity, customer growth, acquisitions, and expansion. The reporting and compliance objectives would focus on meeting regulatory requirements. The bank's managers would then apply the eight components of the COSO risk management framework across all of the organization's levels to align the bank's operations with its risk appetite and strategic objectives.

ERM in Practice

An organization applied the COSO Enterprise Risk Management—Integrated Framework to its cloud-computing program through Google. More than 3 million businesses worldwide are clients of Google's cloud-computing services, which allow data to be stored on shared servers. Although this technology offers many advantages to organizations, it also represents a major change in how organizations operate with associated risks. Additionally, there are different models and service providers for cloud computing. The COSO cube can be transformed into a path for managing the risks at each step of an organization's process for selecting and implementing a cloud-computing option.[12]

[DA11302]

Control Activities

Section 404 of the Sarbanes-Oxley Act states that public companies are required to publish information in their annual reports regarding the scope and adequacy of their internal control structure and procedures for financial reporting. Additionally, the companies are required to assess the effectiveness of these internal controls and procedures. The registered accounting firm that provides an audit of the financial statement is required to attest to and report on the assessment of the effectiveness of the internal control structure and procedures for financial reporting.

Because COSO 2004 historically focused on financial controls and developed its risk management framework in the context of internal audits related to compliance with Sarbanes-Oxley, control activities are a key feature of this standard in comparison with other risk management standards.

Control activities are policies and procedures applied to each of the four categories of objectives—strategic, operations, reporting, and compliance. Overlap may exist in how controls relate to objectives and areas of operation. The most important function of a control is its role in achieving its objective. For example, a control activity may have the objective of ensuring that all bank loans conform to the bank's guidelines. The organization may apply this control activity across regional divisions and branch offices.

Control activities typically have two parts. The first part is the policy that states what should be done, and the second part is the procedure to accomplish the policy. For example, a policy states that all policies should conform to underwriting guidelines. The procedure is to enter all underwriting information into the insurer's computer system and produce daily reports for branch managers, weekly reports for regional managers, and monthly reports for the division vice president.

The risk management process should be monitored to determine the effectiveness of control activities in meeting objectives. There are two types of