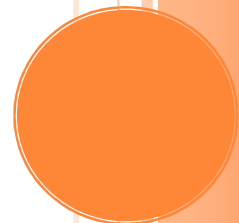




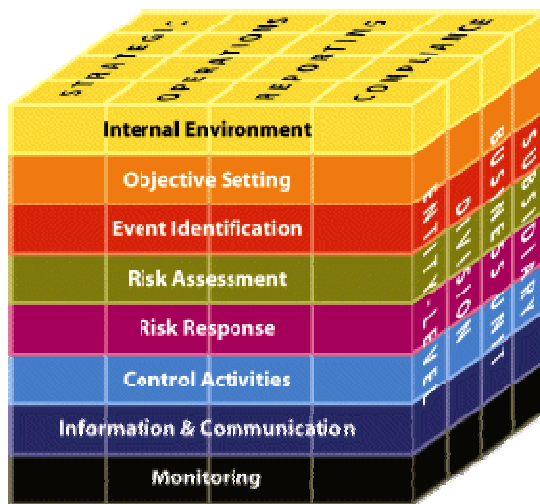
# COSO II: Enterprise Risk Management – Primera Parte

[www.nasaudit.com](http://www.nasaudit.com)

31/07/2009



# COSO II: ENTERPRISE RISK MANAGEMENT – PRIMERA PARTE



Como lo comentamos en uno de nuestros anteriores boletines, existen en la actualidad 2 versiones del Informe COSO. La versión del 1992 y la versión del 2004. La versión del 2004 es una ampliación del Informe original, para dotar al Control Interno de un mayor enfoque hacia el Enterprise Risk Management, o gestión del riesgo.

Es por eso que hoy queremos presentarles el primero de dos artículos relacionados con COSO II Enterprise Risk Management.

Para iniciar queremos mostrar la siguiente ilustración la cual nos enseña la interacción de y posterior descripción de los componentes entre coso I con Coso II, así:



## Componentes de la administración de riesgos – COSO II ERM

### Ambiente interno.

El ambiente interno abarca el tono de una organización y establece la base de cómo el personal de la entidad percibe y trata los riesgos, incluyendo la filosofía de administración de riesgo y el riesgo aceptado, la integridad, valores éticos y el ambiente en el cual ellos operan.

Los factores que se contempla son:

- ✚ Filosofía de la administración de riesgos
- ✚ Apetito al riesgo
- ✚ Integridad y valores éticos
- ✚ Visión del Directorio
- ✚ Compromiso de competencia profesional
- ✚ Estructura organizativa
- ✚ Asignación de autoridad y responsabilidad
- ✚ Políticas y prácticas de recursos humanos

## **Establecimiento de objetivos.**

Los objetivos deben existir antes de que la dirección pueda identificar potenciales eventos que afecten su consecución. La administración de riesgos corporativos asegura que la dirección ha establecido un proceso para fijar objetivos y que los objetivos seleccionados apoyan la misión de la entidad y están en línea con ella, además de ser consecuentes con el riesgo aceptado.

## **Identificación de riesgos.**

Los eventos internos y externos que afectan a los objetivos de la entidad deben ser identificados, diferenciando entre riesgos y oportunidades. Estas últimas revierten hacia la estrategia de la dirección o los procesos para fijar objetivos.

### Técnicas e identificación de riesgos

- ✚ Existen técnicas focalizadas en el pasado y otras en el futuro
- ✚ Existen técnicas de diverso grado de sofisticación
- ✚ Análisis PEST (Factores políticos ó gubernamentales, económicos, tecnológicos y sociales).
- ✚ Análisis DOFA (Debilidades, oportunidades, fortalezas y amenazas)

### Ejemplos:

- ✓ Inventarios de eventos
- ✓ Análisis de información histórica (de la empresa/sector)
- ✓ Indicadores de excepción
- ✓ Entrevistas y cesiones grupales guiadas por facilitadores
- ✓ Análisis de flujos de procesos

Potencialmente los eventos tienen un impacto negativo, positivo ó combinado, representando los primeros riesgos inmediatos, medianos ó de largo plazo, los cuales deben ser evaluados dentro del ERM.

## **Evaluación de riesgos.**

Los riesgos se analizan considerando su probabilidad e impacto como base para determinar cómo deben ser administrados. Los riesgos son evaluados sobre una base inherente y residual bajo las perspectivas de probabilidad (posibilidad de que ocurra un evento) e impacto (su efecto debido a su ocurrencia), con base en datos pasados internos (pueden considerarse de carácter subjetivo) y externos (más objetivos).

## **Respuesta al riesgo.**

La dirección selecciona las posibles respuestas - evitar, aceptar, reducir o compartir los riesgos - desarrollando una serie de acciones para alinearlos con el riesgo aceptado y las tolerancias al riesgo de la entidad.

Las categorías de respuesta al riesgo son:

- ✚ Evitarlo: Se toman acciones de modo de discontinuar las actividades que generan riesgo
- ✚ Reducirlo: Se toman acciones de modo de reducir el impacto, la probabilidad de ocurrencia del riesgo o ambos
- ✚ Compartirlo: Se toman acciones de modo de reducir el impacto o la probabilidad de ocurrencia al transferir o compartir una porción del riesgo
- ✚ Aceptarlo: No se toman acciones que afecten el impacto y probabilidad de ocurrencia del riesgo

En cuanto a la visión del portafolio de riesgos en la respuesta a los mismos, ERM establece:

- ERM propone que el riesgo sea considerado desde una perspectiva de la entidad en su conjunto de riesgos
- Permite desarrollar una visión de portafolio de riesgos tanto a nivel de unidades de negocio como a nivel de la entidad
- Es necesario considerar como los riesgos individuales se interrelacionan

- Permite determinar si el perfil de riesgo residual de la entidad está acorde con su apetito de riesgo global

### **Actividades de control.**

Las políticas y procedimientos se establecen e implantan para ayudar a asegurar que las respuestas a los riesgos se llevan a cabo efectivamente.

### **Información y comunicación**

La información relevante se identifica, captura y comunica en forma y plazo adecuado para permitir al personal afrontar sus responsabilidades. Una comunicación efectiva debe producirse en un sentido amplio, fluyendo hacia abajo, a través, y hacia arriba de la entidad.

### **Monitoreo**

La totalidad de la administración de riesgos corporativos es monitoreada y se efectúan las modificaciones necesarias. Este monitoreo se lleva a cabo mediante actividades permanentes de la dirección, evaluaciones independientes o ambas actuaciones a la vez. La administración de riesgos corporativos no constituye estrictamente un proceso en serie, donde cada componente afecta sólo al siguiente, sino un proceso multidireccional e iterativo en el cual casi cualquier componente puede e influye en otro.

Aquí finalizamos la primera parte del tema COSO II. En nuestro próximo boletín continuaremos con este tema.

Hasta pronto,

### **Equipo de Trabajo Nasaudit**

Aportamos valor a través de nuestro conocimiento.

Bogotá D.C. / Colombia

[info@nasaudit.com](mailto:info@nasaudit.com)

[www.nasaudit.com](http://www.nasaudit.com)