COSO - The Committee of Sponsoring Organizations of the Treadway Commission

Eduardo Martins Pereira (*eduardomartinsp@gmail.com*)
Fernando Bracalente (*bracalente@hotmail.com*)
Marcelo Dinofre (*mdinofre@hotmail.com*)
Mario Luiz Bernardinelli (*mariolb@gmail.com)*

Maio/2008

Abstract

The purpose of this article is to discuss the Committee of Sponsoring Organizations of the Treadway Commission, known as COSO. This discussion will include its origin, short history, and purpose. Also we will introduce some fundamental concepts of COSO as an Enterprise Risk Management framework.

Resumo

O objetivo deste artigo é discutir o ***COSO*** *(The Committee of Sponsoring Organizations of the Treadway Commission)*. Esta discussão apresentará a sua origem, um resumo de sua história e seu objetivo. Além disso, serão apresentados os conceitos fundamentais do ***COSO*** como um modelo de Gerenciamento de Riscos Corporativos.

1. Introdução

Criada originalmente em 1985 nos Estados Unidos, a *National Commission on Fraudulent Financial Reporting* (Comissão Nacional sobre Fraudes em Relatórios Financeiros), também conhecida como *Treadway Commission*[4], foi uma iniciativa independente do setor privado com a finalidade de estudar as causas da ocorrência de fraudes em relatórios financeiros e contábeis e desenvolver recomendações para empresas públicas e seus auditores independentes e para as instituições educativas.

Esta Comissão foi patrocinada por cinco grandes associações de profissionais de classe ligadas à área financeira, sendo totalmente independentes de suas entidades patrocinadoras:

- ***AICPA -*** *American Institute of Certified Public Accounts* (Instituto Americano de Contadores Públicos Certificados)
- ***AAA -*** *American Accounting Association* (Associação Americana de Contadores)
- ***FEI*** - *Financial Executives Internacional* (Executivos Financeiros Internacionais)
- ***IIA*** - *The Insititute of Internal Auditors* (Instituto dos Auditores Internos)
- ***IMA*** - *Institute of Management Accountants* (Instituto dos Contadores Gerenciais)

Em 1992 esta comissão publicou o trabalho *Internal Control – Integrated Framework* (Controle Interno – Um Modelo Integrado), que tornou-se uma referência mundial para o estudo e aplicação dos controles internos.

Posteriormente a Comissão transformou-se em Comitê, passando a ser conhecida como ***COSO*** – *The Committee of Sponsoring Organizations of the Treadway Commission* (Comitê das Organizações Patrocinadoras).

O ***COSO*** é uma entidade sem fins lucrativos, dedicada à melhoria dos relatórios financeiros através da ética, efetividade dos controles internos e governança corporativa.

2. Atendimento à lei Sarbanes-Oxley

Em 2002, após os escândalos das companhias que manipularam suas informações contábeis (*Enron, Tyco, WorldCom* e outras), e que abalaram a confiança dos investidores e reforçaram a necessidade de maior transparência e confiabilidade na confecção e divulgação das informações contábeis e financeiras, o Congresso Americano pressionado pela Sociedade aprovou a Lei *Sarbanes-Oxley*, (Paul S. Sarbanes e Michael Oxley) que reformulou e regulamentou o mercado de capitais, como forma de erradicar a manipulação indevida de informações financeiras.

As mudanças básicas foram nas regras de governança corporativa com o aumento da responsabilidade dos executivos das organizações bem como dos responsáveis perante a emissão e divulgação de relatórios financeiros. Também foi dada mais ênfase no uso de controles internos mais rígidos.

Como decorrência dos fatos apontados, vários estudos foram realizados, procurando identificar as principais falhas nos controles dessas instituições.

Neste cenário, o ***COSO*** identifica os objetivos essenciais do negócio da organização e define controles internos, fornece critérios a partir dos quais os sistemas de controle podem ser avaliados, gera subsídios para que a administração, auditoria e demais interessados possam utilizar, avaliar e validar os controles.

O controle interno é um processo efetuado pelo conselho de administração, executivos ou qualquer outro funcionário de uma organização com a finalidade de possibilitar o máximo de garantia nas seguintes categorias de objetivos:

- **Eficiência e eficácia das operações.** Salvaguarda de seus ativos e prevenção e detecção de fraudes e erros.
- **Confiabilidade das demonstrações financeiras.** Exatidão, integridade e confiabilidade dos registros financeiros e contábeis.
- **Conformidade com as leis e regulamentos vigentes**. Aderência às normas administrativas, às políticas da empresa e à legislação a qual está subordinada.

Ressalta-se que o sistema de controles internos é um instrumento de administração. Apesar de terem o comportamento de processos, os controles internos são avaliados em um ponto específico do tempo e não ao longo do tempo. É nesse ponto, que parte das exigências da Lei *Sarbanes-Oxley* fica atendida.

Observa-se, no entanto, que os controles internos auxiliam na consecução dos objetivos, mas não garantem que eles serão atingidos. Isto ocorre devido, principalmente, a três motivos básicos:

- **Custo/benefício.** Todo controle tem um custo, que deve ser inferior ao custo da consumação do risco que está sendo controlado.
- **Conluio entre pessoas.** As pessoas responsáveis pelos controles, também podem usar de seus conhecimentos para burlar o sistema com objetivos ilícitos em parceria com outros funcionários, clientes ou fornecedores.
- **Eventos externos.** Eventos externos estão além do controle de qualquer organização podendo ser responsáveis por levar um negócio a deixar de alcançar suas metas operacionais ou até mesmo encerrar com as atividades de uma organização.

3. Processo de Controle Interno

O controle interno é um processo constituído de cinco elementos básicos, a saber:

- Ambiente de controle
- Avaliação e gerenciamento de riscos
- Atividades de controle
- Informação e comunicação
- Monitoramento

Conforme descrito anteriormente, o objetivo principal dos controles internos é auxiliar a entidade atingir seus objetivos. Controle interno é um elemento que compõe o processo de gestão.

3.1. Ambiente de controle

Ambiente de controle é uma atitude global da organização, é a disposição, a conscientização e o comportamento de todo o pessoal da empresa a respeito da importância de seus controles e, portanto, envolve o comprometimento dos empregados.

Neste cenário, os funcionários devem ser capazes de saber **o que** deve ser feito, **como** deve ser feito e, finalmente, devem **querer** fazê-lo. A quebra de um destes elos compromete todo o ambiente de controle.

O papel do conselho de administração e da alta gerência é primordial neste cenário: é essencial que fiquem claros:

- Quais são as políticas, procedimentos e o código de conduta a serem adotados.
- A filosofia de funcionamento e de estilo de administração.
- A estrutura organizacional da entidade e os métodos de atribuição de autoridade e responsabilidade.
- A função de auditoria interna, de pessoal, de políticas e procedimentos e segregação de funções.

3.2. Avaliação e gerenciamento de riscos

Os controles internos visam atingir determinados objetivos que, por sua vez, devem ser claros, caso contrário os controles perdem o sentido.

Uma vez estabelecidos os objetivos, deve-se identificar os riscos que possam ameaçar o seu cumprimento e executar as ações necessárias para gerenciá-los.

A avaliação de riscos é um processo de identificação e análise e deverá permitir à entidade identificar as conseqüências pertinentes ao não cumprimento das metas e objetivos operacionais (concretização dos riscos), formando uma base de conhecimento para o seu gerenciamento.

Assim, a avaliação dos riscos é uma atividade pró-ativa que tem por objetivo evitar surpresas desagradáveis á empresa.

O processo de avaliação dos riscos tem que considerar os fatores **internos** e **externos** que podem ter impacto sobre a consecução dos objetivos e devem analisar os riscos e fornecer as bases para o seu manuseio.

3.3. Atividades de controle

Atividades de controle são as atividades executadas durante o processo de execução do trabalho que permite o gerenciamento e a redução dos riscos.

Nesta atividade, são estabelecidos os limites de decisão de cada funcionário, isto é, o funcionário deve saber quais são seus limites operacionais e decisórios e quais transações necessitam de aprovação superior para que seja efetivada. Antes de autorizá-la, ele deve assegurar que todas as informações necessárias a aquela atividade foram executadas. Já os responsáveis pela autorização devem verificar a documentação pertinente.

Atividades de detecção de falhas ou não conformidades devem ser estabelecidas de forma a permitir a confrontação das informações com dados vindos de outras áreas e, se necessário, efetuar as correções necessárias.

Na atividades de controle também se faz a avaliação de adequação e/ou desempenho em relação às metas e objetivos traçados bem como o acompanhamento contínuo do mercado de forma a antecipar desvios que possam ter impacto para a organização.

As atividades de controle também compreendem a segurança física dos ativos, através da implementação de controles de acesso, entrada e saída de materiais, senhas para acesso remoto etc.

Outra atividade de controle é a utilização da segregação de funções, a qual é um método preventivo e de fundamental importância para a eficácia dos resultados dos controles internos adotados.

Por fim, a normatização interna também é uma atividade de controle que visa definir, de maneira formal, as regras internas da organização, que devem ser de fácil acesso para os funcionários e devem definir as responsabilidades, políticas corporativas, fluxos operacionais, funções e procedimentos.

3.4. Informação e comunicação

A comunicação é o fluxo de informações dentro da organização e é essencial para o funcionamento dos controles. A comunicação eficaz ocorre quando esta flui na organização em todas as direções, e quando os empregados recebem informações claras quanto às suas funções e responsabilidades. Uma comunicação eficaz deve ocorrer em todos os níveis da organização.

As informações sobre os planos, ambientes de controle, riscos, atividades de controle e desempenho devem ser transmitidas a todos os funcionários. Já as informações provenientes de entidades externas ou internas, devem ser devidamente identificadas e verificadas quanto a sua confiabilidade e relevância, processadas e transmitidas apenas às pessoas pertinentes ao assunto.

A forma e o prazo em que as informações relevantes são identificadas, colhidas e comunicadas permitem que as pessoas cumpram com suas atribuições. Para identificar, avaliar e responder ao risco, a organização necessita das informações em todos os níveis hierárquicos. A comunicação eficaz ocorre quando esta flui na organização em todas as direções, e quando os empregados recebem informações claras quanto às suas funções e responsabilidades.

Sistemas de informação e elaboração de relatórios contendo informações operacionais, financeiras, e de conformidade, permitem subsidiar a execução e controle das atividades da empresa.

3.5. Monitoramento

Monitoramento é a avaliação dos controles internos ao longo do tempo. É um processo no qual olha-se para a qualidade do desempenho em todos os momentos.

A função do monitoramento é verificar se os controles internos estão adequados e efetivos e pode ser realizado por acompanhamento contínuo das atividades ou por avaliações pontuais.

O monitoramento contínuo é incorporado às atividades normais e repetitivas de uma organização, é conduzida durante a realização da atividade. O monitoramento contínuo é mais eficaz do que as avaliações

pontuais, as quais geralmente ocorrem após a constatação de algum fato (problema).

A profundidade e freqüência do monitoramento dependem da avaliação dos riscos e da eficácia dos procedimentos de fiscalização.

As deficiências identificadas devem ser comunicadas ao mais alto nível da organização.

4. O COSO no Gerenciamento de Riscos Corporativos

Desde a publicação em 1992 do trabalho *Internal Control – Integrated Framework* (Controle Interno – Um Modelo Integrado), o ***COSO*** tornou-se referência para ajudar empresas e outras organizações a avaliar e aperfeiçoar seus sistemas de controle interno, sendo que essa estrutura foi incorporada em políticas, normas e regulamentos adotados por milhares de organizações para controlar melhor suas atividades visando o cumprimento dos objetivos estabelecidos.

Com a preocupação com o gerenciamento de riscos, tornou-se cada vez mais clara a necessidade de uma estratégia sólida, capaz de identificar, avaliar e administrar riscos.

Em 2001, o ***COSO*** iniciou um projeto preocupado com o gerenciamento mais intenso de riscos e solicitou à *Pricewaterhouse Coopers* que desenvolvesse uma estratégia de fácil utilização pelas organizações para avaliar e melhorar o próprio gerenciamento de riscos.

Essa obra, chamada *Enterprise Risk Management Framework* (Gerenciamento de Riscos Corporativos – Estrutura Integrada), ampliou o alcance dos controles internos, oferecendo um enfoque mais vigoroso e abrangente de gerenciamento de riscos corporativos.

4.1. Gerenciamento de Riscos Corporativos

No curso normal dos negócios, as organizações enfrentam incertezas, desafios e uma ampla gama de riscos e o grande desafio da administração é determinar qual é o nível de incerteza ao qual a empresa está preparada para aceitar.

Nem todos os riscos apresentam o mesmo nível de importância. O gerenciamento de riscos corporativos permite aos administradores identificar, avaliar e administrar riscos diante de incertezas, concentrando-se nos riscos de maior impacto – tanto positivo como negativo a fim de agregar valor para os acionistas.

O processo de gerenciamento de riscos é constituído de oito componentes inter-relacionados que integram o modo pelo qual a administração gerencia a organização. Os componentes servem de critério para determinar se o gerenciamento de riscos é eficaz ou não.

Segundo o documento *Gerenciamento de Riscos Corporativos - Estrutura Integrada* o gerenciamento de riscos corporativos requer:

- Alinhar o apetite a risco e a estratégia
- Otimizar as decisões de resposta a risco
- Reduzir surpresas e prejuízos operacionais
- Identificar e administrar os riscos inerentes aos empreendimentos
- Fornecer respostas integradas aos diversos riscos
- Aproveitar as oportunidades
- Melhorar a alocação de capital

O gerenciamento de riscos corporativos é a identificação e análise dos riscos associados ao não cumprimento das metas e objetivos operacionais, de informação e de conformidade, formando uma base de conhecimento que permita definir como estes riscos deverão ser gerenciados.

Os administradores devem definir os níveis de riscos operacionais, de informação e conformidade que estão dispostos a assumir.

A avaliação de riscos é uma responsabilidade da alta administração, mas cabe à auditoria interna fazer uma avaliação própria dos riscos, confrontando-a com a avaliação feita pelos administradores.

A identificação e gerenciamento dos riscos é uma ação pró-ativa.

4.2. Componentes do gerenciamento de riscos corporativos

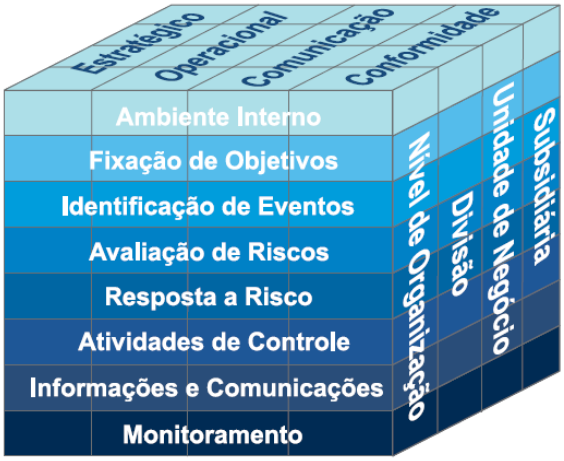
Os oito componentes do gerenciamento de risco corporativos são:

- Ambiente Interno
- Fixação de Objetivos
- Identificação de Eventos
- Avaliação de Riscos
- Resposta a Risco
- Atividades de Controle
- Informações e Comunicações
- Monitoramento

4.3. Relação entre objetivos e componentes

Existe uma relação direta entre os objetivos, que é aquilo que a entidade deseja atingir, e os componentes do gerenciamento de risco que representam o que é necessário para atingir os objetivos. Esta relação está

representada no formato de uma matriz tridimensional, com o aspecto de um cubo, conforme figura a seguir:



O cubo mostra a habilidade que uma entidade tem para focar no gerenciamento de risco corporativo, sendo por categoria de objetivo, componentes de gestão de risco, por unidade de negócio ou por qualquer outro subconjunto.

Em razão da exigência de que a avaliação dos controles internos seja realizada com base em um *framework* reconhecidamente eficaz, o ***COSO*** tornou-se referência para as empresas que, nesse momento, estão em processo de reestruturação ou adaptação de seus ambientes de controle para atender às novas demandas regulatórias.

4.4. O gerenciamento de riscos corporativos e o processo de gestão

O gerenciamento de riscos corporativos é uma das atividades do processo de gestão. Os componentes dessa estrutura são no contexto das ações da direção ao administrar a organização. Observe, porém, que nem todas as atividades da administração fazem parte do gerenciamento de riscos corporativos.

O gerenciamento de riscos corporativos abrange os elementos do processo administrativo que possibilitam à administração tomar decisões. Porém as decisões selecionadas, a partir de uma série de escolhas possíveis, por si só, não são capazes de determinar se o gerenciamento de riscos corporativos está sendo eficaz.

No entanto, mesmo considerando-se que as repostas aos riscos e as atividades de controle selecionadas sejam uma questão de julgamento administrativo, as escolhas devem possibilitar a redução dos riscos a níveis aceitáveis, conforme determinados pelo apetite à risco e à razoável garantia de realização dos objetivos da organização.

4.5. Por dentro dos componentes

Cada um dos componentes do gerenciamento de riscos corporativos definidos pelo ***COSO*** possui características próprias que devem ser bem entendidas.

4.5.1. Ambiente interno

Abrange a cultura da organização, a base para como o risco é visto e dirigido por uma entidade, incluindo a gerencia do risco, a consciência interna sobre risco, a integridade, os valores éticos e o ambiente em que a empresa opera.

4.5.2. Fixação de objetivos

Consiste na identificação e análise de risco externo ou interno que são importantes e podem impactar nos objetivos da empresa. Esta avaliação deve considerar a severidade dos riscos, a freqüência com que estes ocorrem e o seu grau de impacto. Assim a empresa poderá determinar como administrar tais riscos.

4.5.3. Identificação de eventos

A identificação de riscos determina quais riscos podem afetar a organização positivamente ou negativamente.

Eventos de impacto positivo representam oportunidades que são canalizados de volta aos processos e objetivos da organização.

Eventos de impacto negativo representam riscos e exigem avaliação e resposta.

A identificação de eventos de riscos é um processo iterativo porque novos riscos podem ser conhecidos durante a execução da atividade.

4.5.4. Avaliação de riscos

A organização, ao avaliar os riscos, leva em consideração até que ponto os eventos previstos e imprevistos podem impactar na realização de seus objetivos. Em sua análise, leva ainda em consideração a probabilidade e o impacto de sua ocorrência.

Os objetivos da avaliação de riscos são aumentar a probabilidade e o impacto dos eventos positivos e diminuir a probabilidade e o impacto dos eventos adversos (negativos).

Na análise dos riscos, pode-se recorrer à análises qualitativas ou quantitativas dos mesmos. A análise

qualitativa faz a priorização dos riscos através de avaliação e combinação de sua probabilidade de ocorrência e impacto. Já a análise **quantitativa** faz a análise numérica do efeito dos riscos identificados nos objetivos gerais.

4.5.5. Resposta a riscos

A resposta ao risco é o processo de desenvolver e determinar ações para aumentar a produtividade e reduzir as ameaças aos objetivos da organização.

As respostas incluem evitar, reduzir, compartilhar, transferir ou aceitar os riscos.

A administração avalia a probabilidade, o impacto da potencial ocorrência do risco, os custos e benefícios e a prioridade da ação e seleciona então a resposta com a melhor relação dentro das tolerâncias a risco desejadas, inserindo recursos e atividades no orçamento.

A administração identifica as oportunidades que possam existir e obtêm uma visão dos riscos em toda organização, determinando se os riscos residuais gerais são compatíveis com o risco que a organização deseja assumir.

4.5.6. Atividades de controle

As atividades de controle são as respostas aos riscos planejados e definidos nas políticas e procedimentos.

Estas atividades são executadas durante todo o ciclo da atividade que deve ser controlada continuamente para encontrar novos riscos e mudanças nos riscos.

As atividades de controle ocorrem em todos os níveis da organização e compreendem uma série de atividades tais como aprovação, autorização, verificação, reconciliação e revisão do desempenho operacional, da segurança dos bens e da segregação de responsabilidades.

4.5.7. Informação e comunicação

As informações devem ser identificadas, coletadas e comunicadas a tempo de permitir que as pessoas cumpram as suas responsabilidades. Os sistemas de informações da Organização geralmente possuem dados obtidos internamente através de lições aprendidas e também de fontes externas que possibilitam o gerenciamento de riscos e a tomada de decisão.

A comunicação deve atingir todos os níveis da organização. Todo o pessoal da organização recebe da alta administração a mensagem alertando que as responsabilidades do gerenciamento de riscos corporativos devem ser levadas a sério e é uma responsabilidade de todos.

A organização deve estabelecer um plano de comunicações entre os níveis hierárquicos bem como um plano de comunicação com terceiros, clientes, fornecedores, órgãos reguladores e acionistas.

4.5.8. Monitoramento

Os riscos corporativos são monitorados avaliando-se a presença e o funcionamento de seus componentes ao longo do tempo de forma contínua e com avaliações independentes ou mesmo através de uma combinação de ambos.

O monitoramento deve ser contínuo e de forma normal das atividades de administração. As deficiências no gerenciamento de riscos são relatadas aos superiores e as questões mais graves são relatadas ao conselho de administração e à diretoria da organização.

5. Conclusão

Dentro de uma organização, os processos devem ser controlados permitindo assim que qualquer desvio, por menor que seja, possa ser avaliado e corrigido, se necessário.

Para que um processo possa ser controlado, devem ser estabelecidos os meios para que o controle seja efetuado. Mas um controle só tem sentido se o objetivo final for claro e conhecido por todos os envolvidos.

A alta administração deve definir objetivos da organização e passá-los a todos os seus membros e por toda a hierarquia, de forma que fiquem claros e conhecidos.

Como uma organização é composta de muitos processos internos, simultâneos ou não, que se inter-relacionam, se faz necessária a coordenação e o estabelecimento de objetivos para cada um dos mesmos, de forma que o objetivo maior, estabelecido pela alta administração, possa ser atingido.

Eventos, internos ou externos, que podem provocar desvios nos objetivos dos processos podem ocorrer a todo e qualquer momento. Cabe então aos administradores detectar os riscos destes eventos ocorrerem, determinando a probabilidade de sua ocorrência e o impacto que a sua ocorrência teria nos objetivos da organização.

O ***COSO*** é um *framework* que auxilia no estabelecimento dos controles internos e no

gerenciamento dos riscos corporativos. A sua visão corporativa visa oferecer os mecanismos necessários para que os riscos envolvidos na consecução dos objetivos da organização sejam analisados com foco no objetivo principal da organização e não apenas no objetivo do processo em questão.

Referências

[1] GRA – Campinas. Entendendo o COSO. http://www.auditoriainterna.com.br/coso.htm

[2] COSO. The Committee of Sponsoring Organizations. http://www.coso.org

[3]

COSO.http://www.scribd.com/doc/221693/COSO-um-resumo

[4] International Financial Risk Institute. http://riskinstitute.ch/00013184.htm