

Auditoria de Processos

Metodologia COSO

Utilização das “Melhores Práticas em Auditoria”

2012

Auditoria de Processos

Metodologia COSO

1ª Edição

©2012 Clube de Autores

TODOS OS DIREITOS RESERVADOS AO AUTOR. Proibida a Reprodução total ou parcial, por qualquer meio ou processo. Vedada a memorização e/ou recuperação total ou parcial por qualquer sistema de processamento de dados ou imagem e a inclusão de qualquer parte da obra em computador ou meio digital. O titular poderá requerer o cumprimento dos dispositivos legais, incluindo o disposto na Lei nº 9601, de 19 de fevereiro de 1998.

Ficha Catalográfica

Santos, Franklin

Auditoria de Processos - Metodologia COSO / Franklin Santos. – 1ª
Edição. Recife - Ed. Clube de Autores, 2012.

187 p.: Il.

1. Auditoria. 2. Auditoria de Processos.

3. Metodologia COSO 4. Ciência contábil.

I. Título.

Índice para catálogo sistemático

1. Auditoria de Processos - Metodologia COSO: Contabilidade
2. Auditoria Contábil: Ciências Contábeis

Para Aline e Beatriz.

Capítulo 1

COSO

1. COSO

Há uma década, vários profissionais da Auditoria se reuniram em um Comitê, com a intenção de ajudar empresas e outras organizações chamado de COSO (Committee of Sponsoring Organizations of the Treadway Commission) para ajudar empresas e outras organizações a aperfeiçoar e avaliar sistemas de controle interno.

O COSO é formado pela American Accounting Association, American Institute of Certified Public Accountants, Financial Executives International, Institute of Management Accountants e pelo Institute of Internal Auditors, que no Brasil está ligado a AUDIBRA – Instituto dos Auditores Internos do Brasil, através da FLAI – Federação latino-americana de Auditores Internos.

Milhares de organizações passaram a por em prática políticas, normas e regulamentos adotados pelo COSO com a intenção de maior controle de suas atividades.

Nos últimos anos, o foco e a preocupação das organizações passou a ser o gerenciamento de riscos levando a necessidade de uma formatar métodos de identificação, avaliação e administração de riscos.

Em 2001, o “COSO” iniciou um projeto para o desenvolvimento de uma estratégia de fácil utilização pelas organizações com o intuito de avaliar e, gerenciar seus riscos.

Neste período de desenvolvimento, houve uma série de escândalos e quebras de bancos e empresas de grande porte como a Enron, dentre outras, o que gerou prejuízos para investidores, empregados e outras partes interessadas.

Neste contexto ficou clara a necessidade de melhoria nos processos de governança corporativa e no gerenciamento de riscos, além de leis, regulamentos e de padrões a serem seguidos.

Portanto, uma estrutura de gerenciamento de riscos corporativos, com princípios e conceitos fundamentais, além de uma linguagem comum, para o direcionamento e orientação tornou-se muito mais necessária.

O COSO, a partir do seu “Gerenciamento de Riscos Corporativos – Estrutura Integrada” propõe atender esta necessidade, e tem o intuito que a mesma seja adotada por empresas, organizações, e partes interessadas.

Nos EUA surgiram o Ato Sarbanes-Oxley de 2002 e diversas legislações promulgadas em outros países. No caso da Sarbanes-Oxley essa lei amplia a exigência para que companhias abertas tenham sistemas de controle interno, busquem certificação da administração, e contratem Auditoria Independente para atestar a eficácia dos seus controles internos.

O “Gerenciamento de Riscos Corporativos – Estrutura Integrada” oferece um enfoque mais abrangente acerca do gerenciamento de riscos corporativos.

Não é intenção do mesmo substituir a estrutura de controles internos existentes, mas incorporar-se a estrutura existente, atendendo tanto as necessidades de controle interno, bem como estabelecer um processo completo de gerenciamento de riscos.

Capítulo 2

Gerenciamento de riscos

2. Gerenciamento de riscos

O ponto-chave do gerenciamento de riscos corporativos é ratificar que toda organização, independente da sua atividade, existe para gerar algum tipo de valor, seja econômico ou social, às partes interessadas.

As organizações enfrentam incertezas, que desafiam sua administração a determinar até que ponto pode-se aceitar essa incerteza, bem como definir o que esta incerteza resultará no esforço para gerar o valor demandado pelas partes interessadas.

O que chamamos de Incertezas são riscos e oportunidades, que têm potencial agregar valor, ou ameaçar a vida da organização.

A partir do gerenciamento de riscos corporativos os administradores podem identificar as incertezas, os riscos e as oportunidades associadas a sua organização, e a partir disto, precaver-se e melhorar a geração de valor para a organização.

O valor para ser maximizado pela organização deve estabelecer estratégias e objetivos que resultem em um equilíbrio ideal entre metas de crescimento e retorno de investimentos.

A finalidade em se gerenciar riscos é:

- Alinhar o apetite a risco com a estratégia adotada – O apetite a risco significa o quanto determinada organização se dispõe a aceitar ou não determinado risco relacionado à sua atividade operacional.
- Fortalecer as decisões em resposta aos riscos – Identificados e selecionados os riscos mais relacionados à atividade da organização, o próximo passo é estabelecer as decisões da organização como: aceitar o risco, evitar, reduzir, mitigar, ou compartilhar o mesmo.
- Diminuir surpresas e prejuízos operacionais – A partir da identificação dos riscos e de sua estratégia em como lidar com

os mesmos, as organizações passam a ter capacidade em identificar eventuais riscos em potencial e estabelecer prontas respostas aos mesmos.

- Identificação e administração de riscos múltiplos – Qualquer organização enfrenta uma grande quantidade de riscos que afetam a organização em suas diversas áreas, e a gestão dos riscos corporativos traz uma resposta rápida e eficaz aos eventuais impactos, além de responder de forma integrada aos diversos riscos.
- Oportunidades – Os riscos em potencial representam para a organização oportunidades a serem aproveitadas ou evitadas em uma forma proativa.
- Otimização de capital – a identificação dos riscos possibilita à organização avaliar de forma eficaz as necessidades de capital, e conseqüentemente a alocação desse capital.

Todas essas finalidades são inerentes ao gerenciamento de riscos corporativos, e ajudam a organização a alcançar suas metas de desempenho, de lucratividade, e perda de recursos.

Este gerenciamento de riscos corporativos contribui também na comunicação eficaz, no cumprimento de leis, e regulamentos, além de evitar danos à imagem da organização.

Portanto, podemos concluir que a partir do gerenciamento de riscos corporativos a organização pode atingir seus objetivos, evitar perigos, surpresas, e manter uma boa imagem frente aos seus clientes e concorrentes.

2.1. Eventos, Riscos e Oportunidades

Os eventos são situações que ocorrem sem previsão aparente. Os mesmos podem gerar impacto negativo, positivo, ou ambos.

Os de impacto negativo podem impedir a criação de valor ou mesmo destruir o valor existente.

Os de impacto positivo podem contrabalançar os de impacto negativo ou podem representar oportunidades, que por

sua vez representam a possibilidade de um evento ocorrer e influenciar favoravelmente a realização dos objetivos, apoiando a criação ou a preservação de valor.

A direção da organização canaliza as oportunidades para seus processos de elaboração de estratégias ou objetivos, formulando planos que visam ao aproveitamento destes.

2.2. Gerenciamento de Riscos Corporativos

Gerenciamento de riscos corporativos é o processo estabelecido em uma organização a partir de seu conselho de administração, de sua diretoria, e demais empregados aplicando estratégias com o intuito de identificar eventos em potencial, administrar os riscos de modo compatível com o apetite ao risco da organização, possibilitando garantia razoável da continuidade da organização.

Estes são conceitos fundamentais, pois o gerenciamento de riscos corporativos é processo contínuo, conduzido por todos profissionais em todos os níveis da organização, aplicando determinada estratégia, aplicada em toda a organização, em todos os níveis e unidades.

Este gerenciamento permite adequar os níveis de riscos de acordo com o apetite a risco pré-determinado pela organização, conselho de administração, e diretoria executiva, orientando a organização na realização de seus objetivos-fins.

2.3. Realização de Objetivos

A missão ou visão estabelecida por uma organização faz com que sua administração estabeleça planos principais, selecionando estratégias e determinando o alinhamento de seus objetivos nos níveis da organização.

A estrutura do gerenciamento de riscos corporativos é orientada a fim de permitir a organização alcançar seus objetivos e podem ser classificados em quatro categorias:

- Riscos Estratégicos – Dizem respeito às metas gerais, alinhadas com a missão da organização.
- Riscos Operacionais – Dizem respeito à utilização eficaz e eficiente dos recursos à disposição da organização.
- Riscos de Comunicação – Faz-se necessário que as informações de relatórios sejam confiáveis.
- Riscos de Conformidade – O risco que a organização sofre caso não cumpra o que determina a lei e regulamentos aplicáveis.

Esta classificação enfoca os aspectos distintos do gerenciamento de riscos de uma organização.

Apesar de categorias distintas, as mesmas estão relacionadas, pois uma vez que determinado objetivo pode ser classificado em mais de uma categoria, tratam de necessidades diferentes da organização e podem permanecer sob a responsabilidade direta de diferentes executivos.

A realização da estratégia da organização está sujeita a eventos externos, que nem sempre estão sob o controle da organização, como elevação da taxa de inflação, enchentes.

Neste sentido o gerenciamento de riscos corporativos é capaz de proteger a organização, já que a diretoria executiva e o conselho de administração, na função de controle, e supervisão poderão ficar bem informados, e se precaver, ou se antecipar, para que os objetivos da organização sejam alcançados, ou pelo menos pouco atingidos por eventos externos.

2.4. Componentes do Gerenciamento de Riscos Corporativos

O gerenciamento de riscos corporativos é composto por oito componentes inter-relacionados, pela qual a administração gerência a organização, e estão integrados com o processo de gestão. Esses componentes são:

- Ambiente Interno – o ambiente interno compreende o que a organização, a partir da diretoria executiva, conselho de administração, e demais funcionários, que fornecem a base

pela qual os riscos são identificados e abordados pelo seu pessoal, inclusive para a definição da filosofia de gerenciamento de riscos a ser tomada, o apetite ao risco que a organização se expõe, à integridade, e os valores éticos inerentes a organização.

- **Fixação de Objetivos** – os objetivos devem ser definidos antes pela administração, para que a mesma possa identificar eventos em potencial que poderão afetar a sua continuidade. O gerenciamento de riscos corporativos, portanto, passa a ser um processo implementado para estabelecer objetivos, e metas que dêem suporte e alinhem a missão da organização e sejam compatíveis com o seu apetite a riscos.
- **Identificação de Eventos** – Eventos internos e externos influenciam o andamento no cumprimento dos objetivos de uma organização, e devem ser identificados e classificados como riscos ou oportunidades. As oportunidades identificadas serão canalizadas para o estabelecimento de estratégias da administração com o intuito do atingimento de seus objetivos, e metas.
- **Avaliação de Riscos** – Os riscos detectados serão analisados, levando-se em consideração sua probabilidade e o impacto esperado para servir de base na determinação do modo pelo qual deverão ser administrados.
- **Resposta a Risco** – A administração escolherá como irá responder aos riscos, se evitará, ou aceitará, ou ignorá-lo, reduzindo ou compartilhando, através de várias medidas para alinhar os riscos, a sua tolerância, e apetite a risco.
- **Atividades de Controle** – O Controle pressupõe políticas e procedimentos estabelecidos para assegurar que as respostas aos riscos sejam executadas com eficácia.
- **Informações e Comunicações** – Informações relevantes serão identificadas, colhidas e comunicadas de forma, e prazo permitindo que a administração se proteja da melhor

forma aos impactos. A comunicação, por sua vez, fará com que a informação flua a todos os níveis da organização.

- **Monitoramento** – O monitoramento da gestão de riscos é feita por atividades de gerenciamento contínuo, avaliações independentes, e quando necessária à integridade da gestão de riscos corporativos são realizadas modificações necessárias.

O gerenciamento de riscos corporativos, portanto, não é um processo em série pelo qual um componente afeta apenas o próximo.

O processo é multidirecional, interagindo entre todos os componentes e influenciando um aos outros.

2.5. Objetivos e Componentes

Toda organização tem objetivos a serem alcançados, e os componentes do gerenciamento de riscos corporativos têm relação direta com estes objetivos, o que faz com que essa relação possa ser representada por uma matriz tridimensional em forma de cubo.



Fonte: COSO

As quatro categorias de objetivos (os estratégicos, os operacionais, os de comunicação e os de conformidade) estão representadas nas colunas verticais.

Os oito componentes nas linhas horizontais e as unidades de uma organização na terceira dimensão, todos em interação.

Essa representação gráfica ilustra a capacidade de manter o enfoque na totalidade do gerenciamento de riscos de uma organização, ou na categoria de objetivos, componentes, unidade da organização ou qualquer um dos subconjuntos.

2.7. Eficácia

O grau de eficácia do gerenciamento de riscos corporativos de uma organização vai ser avaliado a partir de uma série de julgamentos decorrentes da avaliação da presença e da eficácia do funcionamento de cada um dos oito componentes da estrutura COSO (Cubo COSO).

Como podemos ver os componentes do “COSO” também são critérios para o gerenciamento eficaz de riscos corporativos.

Para que os componentes estejam presentes e funcionem de forma satisfatória, não poderá haver fraquezas significantes em cada componente, e os riscos que porventura apareçam necessitarão estar enquadrados no apetite a risco da organização.

Caso o gerenciamento de riscos corporativos seja eficaz em cada uma das quatro categorias de objetivos, isto significará que a diretoria executiva, e o conselho de administração terão razoável certeza que objetivos estratégicos e operacionais estão realmente sendo alcançados.

Além disso, saberão que o sistema de comunicação da empresa está sendo confiável, e que todas leis e regulamentos cabíveis estão sendo cumpridos.

Importante salientar que os oito componentes COSO não funcionarão igualmente para todas as organizações. A aplicação em organizações de pequeno e médio portes, por exemplo, poderá ser implementada de forma menos formal, ou menos estruturada.

2.8. Limitações

Apesar de oferecer importantes benefícios, o gerenciamento de riscos corporativos está sujeito a limitações.

As limitações partem do princípio que o julgamento humano, no processo decisório, pode ser falho, as decisões de respostas a risco e o estabelecimento dos controles necessitam levar em conta os custos e benefícios relativos.

Falhas por erro ou engano humano, controles anulados por conluio entre duas ou mais pessoas, e a administração tem o poder de recusar-se a aceitar as decisões de gestão de riscos.

Estas limitações impedirão que o conselho de administração e a diretoria executiva tenham absoluta garantia da realização dos objetivos da organização.

2.9. Abrangência do Controle Interno

O controle interno faz parte do gerenciamento de riscos corporativos. A estrutura do gerenciamento de riscos corporativos abrange o controle interno.

O controle interno é definido e descrito sob o título “Controle Interno – Estrutura Integrada”. Em razão do fato da estrutura ter resistido ao tempo e ser base das normas, dos regulamentos e das leis existentes, o documento permanece vigente como fonte de definição e marco para as estruturas de controles internos.

Capítulo 3

Funções e Responsabilidades

3. Funções e Responsabilidades

Cada um dos colaboradores em uma organização tem uma parcela de responsabilidade no gerenciamento de riscos corporativos.

O presidente executivo é o principal responsável e tem a missão de assumir a responsabilidade da iniciativa.

Cabe aos demais diretores executivos apoiar a filosofia de administração de riscos da organização, incentivar a observação de seu apetite a risco e administrar os riscos dentro de suas esferas de responsabilidade, conforme as tolerâncias a risco.

Normalmente a responsabilidade fundamental de suporte cabe ao diretor de riscos, diretor-financeiro, auditor interno e outros.

Os outros membros da organização são responsáveis pela execução do gerenciamento de riscos em cumprimento das diretrizes e dos protocolos estabelecidos.

A supervisão do gerenciamento de riscos fica a cargo do conselho de administração, sempre ciente e de acordo com o grau de apetite a risco da organização.

As diversas partes externas como clientes, revendedores, parceiros comerciais, auditores externos, agentes normativos e analistas financeiros frequentemente fornecem informações úteis para a condução do gerenciamento de riscos, porém não são responsáveis pela sua eficácia e nem fazem parte do gerenciamento de riscos da organização.

3.1. Organização do Relatório

O relatório deve ser apresentado em dois volumes. O primeiro volume contém a “Estrutura e este o Resumo Executivo”. A

“Estrutura” irá definir o gerenciamento de riscos da organização e descrever os princípios, conceitos, fornecendo instruções a todos os níveis executivos de empresas e outras organizações, quanto ao seu uso na avaliação e no aprimoramento da eficácia do gerenciamento de riscos corporativos.

O “Resumo Executivo” é uma visão geral, dirigida aos presidentes, diretores executivos, membros do conselho de administração e agentes normativos.

O segundo volume, “Técnicas de Aplicação” ilustra as técnicas úteis de aplicação dos elementos da estrutura.

3.2.Utilização do Relatório

As ações recomendadas, que podem ser interpretadas como resultado do relatório depende da posição e da função das partes envolvidas:

- Conselho de Administração – O conselho deverá discutir com a alta administração a situação do gerenciamento de riscos da organização e fornecer a supervisão necessária. O conselho deve certificar-se que esteja ciente dos riscos mais significativos, em conjunto com as ações que a diretoria executiva esteja realizando, e da forma em que está assegurando um gerenciamento de riscos eficaz. O conselho deve considerar a possibilidade de obter a opinião de auditores internos e externos.
- Alta Administração – O presidente executivo deve reunir as gerências das unidades de negócios e funcionários essenciais para discutir uma avaliação inicial das funcionalidades de gestão de riscos da organização e de sua eficácia. Qualquer que seja a sua forma, a avaliação inicial deverá determinar se existe necessidade de uma avaliação mais ampla e profunda e como conduzi-la.

- Outros Profissionais da Organização – Cabem aos diretores e demais empregados avaliar como estão conduzindo suas responsabilidades à luz desta estrutura, e discutir com seus superiores formas de como fortalecer o gerenciamento de riscos da organização. Os auditores internos devem levar em conta a amplitude de seu enfoque no que se refere à gestão dos riscos corporativos.
- Agentes Normativos – A presente estrutura possibilita uma visão compartilhada do gerenciamento de riscos da organização, inclusive daquilo que ela pode fazer e suas limitações. Os agentes normativos podem consultar essa estrutura ao estabelecer expectativas, por meio de normas, orientações ou aplicação de exames para as organizações supervisoras.
- Organizações Profissionais – Organizações normativas e outras organizações profissionais, que oferecem orientações sobre administração financeira, auditoria ou tópicos relacionados, devem considerar os seus padrões e as orientações à luz dessa estrutura. Quanto menor for a diversidade de conceitos e terminologia, maior será o benefício a todos os agentes envolvidos.
- Educadores – Essa estrutura pode tornar-se motivo de pesquisa e análise acadêmicas para identificar os pontos que podem ser aprimorados no futuro.

Todos os componentes da organização, conforme seu nível estratégico deverá utilizar uma linguagem comum e comunicar-se, dessa forma, com maior eficácia.

Os executivos terão, portanto, como avaliar o processo de gestão de riscos corporativos de suas próprias organizações em relação a um padrão, como fator de comparabilidade, e fortalecer o

processo, conduzindo a organização rumo aos objetivos e metas estabelecidos.

No caso de legisladores e dos agentes reguladores, os mesmos poderão adquirir maior entendimento do gerenciamento de riscos corporativos, além de ter uma melhor compreensão de seus benefícios e de suas limitações.

Assim, as organizações estão em contato constante com incertezas, riscos, com isso, a administração tem de calcular o nível de incerteza que a organização poderá aceitar, no intuito de maximizar a agregação de valor as suas diversas partes interessadas.

O gerenciamento de riscos corporativos permite identificar, avaliar, e administrar riscos, além de integrar o processo de agregação, a partir da criação e preservação de valor.

O gerenciamento de riscos corporativos é processo integrado pelo conselho de administração, pela diretoria executiva e pelos demais colaboradores, aplicado no estabelecimento de estratégias a serem postas em prática em toda a organização.

Além de identificar eventos em potencial, capazes de afetar a organização, o processo permite o gerenciamento de riscos de forma a cobrir o apetite a risco estabelecido pela organização e, ainda, possibilitar a execução de seus objetivos.

O processo, baseado no COSO, e como já explicado anteriormente é constituído de oito componentes inter-relacionados e integram o modo pelo qual a administração gerencia a organização.

Estes componentes estão associados e servem de critério para determinar se o gerenciamento de riscos é eficaz ou não.

Um dos objetivos fundamentais dessa estrutura é a contribuição para a gestão de empresas e demais organizações, na medida em que as mesmas adotem uma forma mais adequada de abordar os riscos inerentes ao cumprimento de seus objetivos.

Porém, o significado de gestão de riscos corporativos irá variar de pessoa para pessoa e o processo pode receber diversos rótulos e significados, o que constitui em obstáculo ao entendimento comum.