COSO

Gerenciamento de Riscos Corporativos - Estrutura Integrada

Sumário Executivo
Estrutura

PRICEWATERHOUSECOOPERS

COSO

Gerenciamento de Riscos Corporativos - Estrutura Integrada

Sumário Executivo
Estrutura

Committee of Sponsoring Organizations of the Treadway Commission (COSO)

Supervisão	Representante
Presidência do COSO	John J. Flaherty
American Accounting Association	Larry E. Rittenberg
American Institute of Certified Public Accountants	Alan W. Anderson
Financial Executives International	John P. Jessup Nicholas S. Cyprus
Institute of Management Accountants	Frank C. Minter Dennis L. Neider
The Institute of Internal Auditors	William G. Bishop, III David A. Richards

Conselho Consultivo do COSO para o Projeto

Orientação

Tony Maki
Sócio
Moss Adams LLP

Mark S. Beasley
Professor Catedrático
North Carolina State University

Jerry W. DeFoor
Vice-presidente e Controller
Protective Life Corporation

James W. DeLoach
Diretor Administrativo
Protiviti Inc.

Andrew J. Jackson
Vice-presidente Sênior de Enterprise Risk Assurance Services
American Express Company

Steven E. Jameson
Vice-presidente Executivo, Responsável pela Auditoria Interna e Responsável pelo Setor de Riscos do Community Trust Bancorp, Inc.

John P. Jessup
Vice Presidente e Tesoureiro E. I. duPont de Nemours and Company

Tony M. Knapp
Vice-presidente Sênior e Controller
Motorola, Inc.

Douglas F. Prawitt
Professor Catedrático
Brigham Young University

PricewaterhouseCoopers LLP

Autor
Principais Colaboradores

Richard M. Steinberg
Ex-sócio e Líder de Exercício de Autoridade Corporativa (Atualmente Steinberg Consultores de Exercício de Autoridade)

Frank J. Martens
Gerente Sênior, Serviços a Clientes
Vancouver, Canadá

Miles E.A. Everson
Sócio e Serviços Financeiros
Finanças, Operações, Líder do Setor de Riscos e Conformidade
New York, EUA

Lucy E. Nottingham
Gerente, Serviços Internos de Empresa
Boston, EUA

Prefácio

Há mais de uma década, o Committee of Sponsoring Organizations of the Treadway Commission (COSO) publicou a obra *Internal Control – Integrated Framework* para ajudar empresas e outras organizações a avaliar e aperfeiçoar seus sistemas de controle interno. Desde então, a referida estrutura foi incorporada em políticas, normas e regulamentos adotados por milhares de organizações para controlar melhor suas atividades visando o cumprimento dos objetivos estabelecidos.

Nos últimos anos, intensificou-se o foco e a preocupação com o gerenciamento de riscos, e tornou-se cada vez mais clara a necessidade de uma estratégia sólida, capaz de identificar, avaliar e administrar riscos. Em 2001, o "COSO[1]" iniciou um projeto com essa finalidade e solicitou à PricewaterhouseCoopers que desenvolvesse uma estratégia de fácil utilização pelas organizações para avaliar e melhorar o próprio gerenciamento de riscos.

O período de desenvolvimento dessa estrutura foi marcado por uma série de escândalos e quebras de negócios de grande repercussão, que gerou prejuízos de grande monta a investidores, empregados e outras partes interessadas. Na esteira desses eventos, vieram solicitações de melhoria dos processos de governança corporativa e gerenciamento de riscos, por meio de novas leis, regulamentos e de padrões a serem seguidos. A necessidade de uma estrutura de gerenciamento de riscos corporativos, capaz de fornecer os princípios e conceitos fundamentais, com uma linguagem comum, direcionamento e orientação claros, tornou-se ainda mais necessária. O COSO é da opinião que a presente obra "Gerenciamento de Riscos Corporativos – Estrutura Integrada" vem para preencher essa lacuna e espera que ela seja amplamente adotada pelas empresas e por outras organizações, bem como por todas as partes interessadas.

Nos Estados Unidos, entre as conseqüências, destacam-se o Ato Sarbanes-Oxley de 2002 e a legislação semelhante que está sendo promulgada ou analisada em outros países. Essa lei amplia a exigência de que as companhias abertas mantenham sistemas de controle interno, demandem a certificação da administração e contratem os serviços de auditores independentes para atestar a eficácia dos referidos sistemas. A obra *Internal Control – Integrated Framework*, que vem sendo submetida ao teste do tempo, serve como norma de ampla aceitação para o atendimento dos requisitos de comunicação.

A obra "Gerenciamento de Riscos Corporativos – Estrutura Integrada", amplia seu alcance em controles internos, oferecendo um enfoque mais vigoroso e extensivo no tema mais abrangente de gerenciamento de riscos corporativos. A presente estrutura de gerenciamento de riscos corporativos, embora não tenha por meta substituir a estrutura de controles internos das organizações, incorpor a estrutura de controle interno em seu conteúdo e, a poderá ser por estas utilizada, tanto para atender às suas necessidades de controle interno quanto para adotar um processo completo de gerenciamento de riscos.

Entre os principais críticos às administrações está a determinação da extensão do risco que a organização está preparada para enfrentar e disposta a aceitar na medida em que se empenha para agregar valor. A presente publicação possibilitará melhores condições para enfrentar esse desafio.

John J. Flaherty
Presidente, Coso

Tony Maki
Presidente do Conselho Consultivo

[1] "COSO" The Committee of Sponsoring Organizations of the Treadway Commission

Introdução à edição brasileira

Temos a satisfação de apresentar ao público de língua portuguesa, a tradução da versão original em inglês da publicação “Gerenciamento de Riscos Corporativos – Estrutura Integrada” emitido pelo Committee of Sponsoring Organization of the Treadway Commission (COSO) com a colaboração da PricewaterhouseCoopers.

Essa publicação tem o objetivo de ser considerado como um modelo conceitual para o gerenciamento de riscos corporativos, proporcionando as diretrizes para a evolução e aprimoramento do gerenciamento de riscos e dos procedimentos para sua análise.

O COSO é formado por representantes da American Accounting Association, American Institute of Certified Public Accountants, Financial Executives Internationl, Institute of Managements Accountants e pelo Institute of Internal Auditors, ao qual está ligado a AUDIBRA – Instituto dos Auditores Internos do Brasil, através da FLAI – Federação latino-americana de Auditores Internos.

A AUDIBRA, juntamente com a PricewaterhouseCoopers prepararam a presente publicação destinada aos profissionais de auditoria interna, auditoria externa, gerenciamento de riscos, controles internos, órgãos reguladores, conselheiros e administradores em geral visando difundir os conceitos de riscos corporativos definidos pelo Comitê Consultivo do COSO.

A primeira parte contém o sumário executivo e a estrutura, onde são descritos os componentes essenciais do gerenciamento de riscos corporativos, seus princípios e conceitos-chave, possibilitando uma linguagem comum. A segunda parte contém as técnicas de aplicação, descrevendo exemplos relacionados com cada um dos componentes, de forma a facilitar sua aplicação. Também são apresentados os elementos de controle interno anteriormente descritos pelo COSO no ano de 1992, ampliando o componente de avaliação de riscos, considerando que para que haja gerenciamento de riscos corporativos seja eficaz, deve existir controles internos efetivos.

Finalmente, agradecemos aos profissionais da AUDIBRA e da PricewaterhouseCoopers que através de seu esforço e dedicação, tornaram essa tradução possível.

Rogério Roberto Gollo
Sócio da PricewaterhouseCoopers
Governance, Risk and Compliance

Oswaldo Basile
Presidente
AUDIBRA – Instituto dos Auditores Internos do Brasil

Sumário

COSO

Gerenciamento de Riscos Corporativos - Estrutura Integrada

Sumário Executivo

Sumário Executivo

A premissa inerente ao gerenciamento de riscos corporativos é que toda organização existe para gerar valor às partes interessadas. Todas as organizações enfrentam incertezas, e o desafio de seus administradores é determinar até que ponto aceitar essa incerteza, assim como definir como essa incerteza pode interferir no esforço para gerar valor às partes interessadas. Incertezas representam riscos e oportunidades, com potencial para destruir ou agregar valor. O gerenciamento de riscos corporativos possibilita aos administradores tratar com eficácia as incertezas, bem como os riscos e as oportunidades a elas associadas, a fim de melhorar a capacidade de gerar valor.

O valor é maximizado quando a organização estabelece estratégias e objetivos para alcançar o equilíbrio ideal entre as metas de crescimento e de retorno de investimentos e os riscos a elas associados, e para explorar os seus recursos com eficácia e eficiência na busca dos objetivos da organização. O gerenciamento de riscos corporativos tem por finalidade:

- Alinhar o apetite a risco com a estratégia adotada – os administradores avaliam o apetite a risco da organização ao analisar as estratégias, definindo os objetivos a elas relacionados e desenvolvendo mecanismos para gerenciar esses riscos.
- Fortalecer as decisões em resposta aos riscos – o gerenciamento de riscos corporativos possibilita o rigor na identificação e na seleção de alternativas de respostas aos riscos - como evitar, reduzir, compartilhar e aceitar os riscos.
- Reduzir as surpresas e prejuízos operacionais – as organizações adquirem melhor capacidade para identificar eventos em potencial e estabelecer respostas a estes, reduzindo surpresas e custos ou prejuízos associados.
- Identificar e administrar riscos múltiplos e entre empreendimentos – toda organização enfrenta uma gama de riscos que podem afetar diferentes áreas da organização. A gestão de riscos corporativos possibilita uma resposta eficaz a impactos inter relacionados e, também, respostas integradas aos diversos riscos.
- Aproveitar oportunidades – pelo fato de considerar todos os eventos em potencial, a organização posiciona-se para identificar e aproveitar as oportunidades de forma proativa.
- Otimizar o capital – a obtenção de informações adequadas a respeito de riscos possibilita à administração conduzir uma avaliação eficaz das necessidades de capital como um todo e aprimorar a alocação desse capital.

Essas qualidades, inerentes ao gerenciamento de riscos corporativos ajudam os administradores a atingir as metas de desempenho e de lucratividade da organização, e evitam a perda de recursos. O gerenciamento de riscos corporativos contribui para assegurar comunicação eficaz e o cumprimento de leis e regulamentos, bem como evitar danos à reputação da organização e suas conseqüências. Em suma, o gerenciamento de riscos corporativos ajuda a organização a atingir seus objetivos e a evitar os perigos e surpresas em seu percurso.

Eventos – Riscos e Oportunidades

Os eventos podem gerar impacto tanto negativo quanto positivo ou ambos. Os que geram impacto negativo representam riscos que 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.

Definição de Gerenciamento de Riscos Corporativos

O gerenciamento de riscos corporativos trata de riscos e oportunidades que afetam a criação ou a preservação de valor, sendo definido da seguinte forma:

> O gerenciamento de riscos corporativos é um processo conduzido em uma organização pelo conselho de administração, diretoria e demais empregados, aplicado no estabelecimento de estratégias, formuladas para identificar em toda a organização eventos em potencial, capazes de afetá-la, e administrar os riscos de modo a mantê-los compatível com o apetite a risco da organização e possibilitar garantia razoável do cumprimento dos seus objetivos.

Essa definição reflete certos conceitos fundamentais. O gerenciamento de riscos corporativos é:

- um processo contínuo e que flui através da organização;
- conduzido pelos profissionais em todos os níveis da organização;
- aplicado à definição das estratégias;
- aplicado em toda a organização, em todos os níveis e unidades, e inclui a formação de uma visão de portfólio de todos os riscos a que ela está exposta;
- formulado para identificar eventos em potencial, cuja ocorrência poderá afetar a organização, e para administrar os riscos de acordo com seu apetite a risco;
- capaz de propiciar garantia razoável para o conselho de administração e a diretoria executiva de uma organização;
- orientado para a realização de objetivos em uma ou mais categorias distintas, mas dependentes.

Essa definição é intencionalmente ampla e adota conceitos fundamentais sobre a forma como as empresas e outras organizações administram riscos, possibilitando uma base para sua aplicação em organizações, indústrias e setores. O gerenciamento de riscos corporativos orienta seu enfoque diretamente para o cumprimento dos objetivos estabelecidos por uma organização específica e fornece parâmetros para definir a eficácia desse gerenciamento de riscos.

Realização de Objetivos

Com base na missão ou visão estabelecida por uma organização, a administração estabelece os planos principais, seleciona as estratégias e determina o alinhamento dos objetivos nos níveis da organização. Essa estrutura de gerenciamento de riscos corporativos é orientada a fim de alcançar os objetivos de uma organização e são classificados em quatro categorias:

- Estratégicos – metas gerais, alinhadas com o que suportem à sua missão.
- Operações – utilização eficaz e eficiente dos recursos.
- Comunicação – confiabilidade de relatórios.
- Conformidade – cumprimento de leis e regulamentos aplicáveis.

Essa classificação possibilita um enfoque nos aspectos distintos do gerenciamento de riscos de uma organização. Apesar de essas categorias serem distintas, elas se inter-relacionam, 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. Essa classificação também permite diferenciar o que pode ser esperado de cada categoria de objetivos. A salvaguarda dos recursos, outra categoria utilizada por algumas organizações, também é descrita.

Em razão do fato dos objetivos relacionados com a confiabilidade de relatórios e o cumprimento de leis e regulamentos estarem sob controle da organização, pode-se esperar que o gerenciamento de riscos corporativos forneça uma garantia razoável em relação ao atendimento desses objetivos. Entretanto, a realização de objetivos estratégicos e operacionais está sujeita à ação de eventos externos nem sempre sob o controle da organização; da mesma forma, em relação a esses objetivos, o gerenciamento de riscos corporativos é capaz de propiciar uma garantia razoável que a diretoria executiva e o conselho de administração, na função de supervisão, serão informados, no momento adequado, o quanto a organização está avançando na direção do atendimento dos objetivos.

Componentes do Gerenciamento de Riscos Corporativos

O gerenciamento de riscos corporativos é constituído de 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 tom de uma organização e fornece a base pela qual os riscos são identificados e abordados pelo seu pessoal, inclusive a filosofia de gerenciamento de riscos, o apetite a risco, a integridade e os valores éticos, além do ambiente em que estes estão.

- Fixação de Objetivos – os objetivos devem existir antes que a administração possa identificar os eventos em potencial que poderão afetar a sua realização. O gerenciamento de riscos corporativos assegura que a administração disponha de um processo implementado para estabelecer os objetivos que propiciem suporte e estejam alinhados com a missão da organização e sejam compatíveis com o seu apetite a riscos.

- Identificação de Eventos – os eventos internos e externos que influenciam o cumprimento dos objetivos de uma organização devem ser identificados e classificados entre riscos e oportunidades. Essas oportunidades são canalizadas para os processos de estabelecimento de estratégias da administração ou de seus objetivos.

- Avaliação de Riscos – os riscos são analisados, considerando-se a sua probabilidade e o impacto como base para determinar o modo pelo qual deverão ser administrados. Esses riscos são avaliados quanto à sua condição de inerentes e residuais.

- Resposta a Risco – a administração escolhe as respostas aos riscos - evitando, aceitando, reduzindo ou compartilhando - desenvolvendo uma série de medidas para alinhar os riscos com a tolerância e com o apetite a risco.

- Atividades de Controle – políticas e procedimentos são estabelecidos e implementados para assegurar que as respostas aos riscos sejam executadas com eficácia.

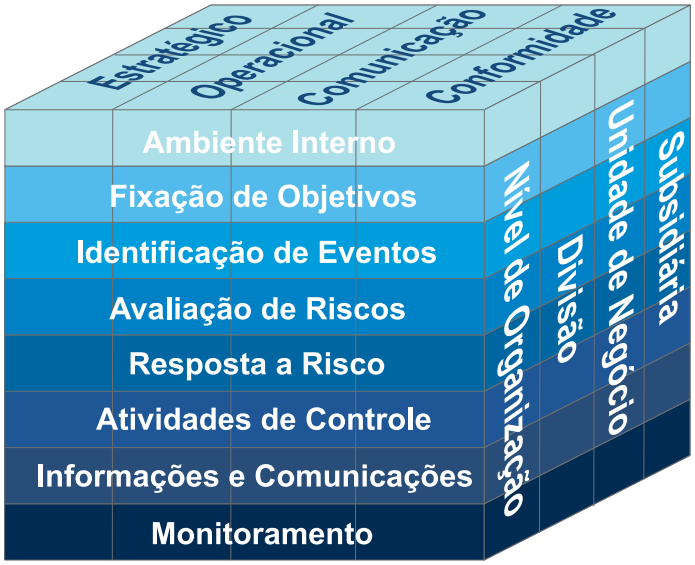
- Informações e Comunicações – as informações relevantes são identificadas, colhidas e comunicadas de forma e no prazo que permitam que cumpram suas responsabilidades. A comunicação eficaz também ocorre em um sentido mais amplo, fluindo em todos níveis da organização.

- Monitoramento – a integridade da gestão de riscos corporativos é monitorada e são feitas as modificações necessárias. O monitoramento é realizado através de atividades gerenciais contínuas ou avaliações independentes ou de ambas as formas.

A rigor, o gerenciamento de riscos corporativos não é um processo em série pelo qual um componente afeta apenas o próximo. É um processo multidirecional e interativo segundo o qual quase todos os componentes influenciam os outros.

Relacionamento entre Objetivos e Componentes

Existe um relacionamento direto entre os objetivos, que uma organização empenha-se em alcançar, e os componentes do gerenciamento de riscos corporativos, que representam aquilo que é necessário para o seu alcance. Esse relacionamento é apresentado em uma matriz tridimensional em forma de cubo.



As quatro categorias de objetivos (estratégicos, operacionais, de comunicação e conformidade) estão representadas nas colunas verticais. Os oito componentes nas linhas horizontais e as unidades de uma organização na terceira dimensão. Essa representação 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.

Eficácia

A determinação do grau de eficácia do gerenciamento de riscos corporativos de uma organização corresponde ao julgamento decorrente da avaliação da presença e da eficácia do funcionamento dos oito componentes. Desse modo, os componentes também são critérios para o gerenciamento eficaz de riscos corporativos. Para que os componentes possam estar presentes e funcionar adequadamente, não poderá haver fraquezas significantes, e os riscos necessitam ser enquadrados no apetite a risco da organização.

Quando se constata que o gerenciamento de riscos corporativos é eficaz em cada uma das quatro categorias de objetivos, isso significa que o conselho de administração e a diretoria executiva terão garantia razoável de que entenderam até que ponto, os objetivos estratégicos e operacionais não estão realmente sendo alcançados, o sistema de comunicação da empresa é confiável, e todas as leis e regulamentos cabíveis estão sendo observados.

Os oito componentes não funcionarão de forma idêntica em todas as organizações. A sua aplicação em organizações de pequeno e médio portes, por exemplo, poderá ser menos formal e menos estruturada. Não obstante, as pequenas organizações podem apresentar um gerenciamento de riscos eficaz, desde que cada um de seus componentes esteja presente e funcionando adequadamente.

Limitações

A despeito de oferecer importantes benefícios, o gerenciamento de riscos corporativos está sujeito a limitações. Além dos fatores discutidos anteriormente, as limitações originam-se do fato de 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. Podem ocorrer falhas causadas por erro ou engano humano, os controles podem ser 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. Essas limitações impedem que o conselho de administração e a diretoria executiva tenham absoluta garantia da realização dos objetivos da organização.

Abrangência do Controle Interno

O controle interno é parte integrante do gerenciamento de riscos corporativos. A estrutura do gerenciamento de riscos corporativos abrange o controle interno, originando dessa forma uma conceituação e uma ferramenta de gestão mais eficiente. 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. Enquanto que apenas algumas porções do texto de “Controle Interno – Estrutura Integrada” estão sendo reproduzidas na presente estrutura, a sua totalidade da mesma está incorporada como referência.

Funções e Responsabilidades

Cada um dos empregados de uma organização tem uma parcela de responsabilidade no gerenciamento de riscos corporativos. O presidente-executivo é o principal responsável e deve assumir a responsabilidade da iniciativa. Cabe aos outros 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. Via de regra, cabe ao diretor de riscos, diretor-financeiro, auditor interno e outros, responsabilidades fundamentais de suporte. Os outros membros da organização são responsáveis pela execução do gerenciamento de riscos em cumprimento das diretrizes e dos protocolos estabelecidos. O conselho de administração executa importante atividade de supervisão do gerenciamento de riscos da organização, estando ciente e de acordo com o grau de apetite a risco da organização. Diversas partes externas, como clientes, revendedores, parceiros comerciais, auditores externos, agentes normativos e analistas financeiros freqüentemente 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.

Organização do Presente Relatório

Este relatório é apresentado em dois volumes. O primeiro volume contém a “Estrutura e este o Resumo Executivo”. A “Estrutura” define o gerenciamento de riscos da organização e descreve seus princípios e 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.

Utilização do Presente Relatório

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

- Conselho de Administração – O conselho deve 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, bem como de outros.
- Alta Administração – Esse estudo recomenda que o presidente-executivo avalie as funcionalidades de administração de riscos da organização. Em uma abordagem, o presidente-executivo reúne as gerencias 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 – Cabe 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. Assumindo-se que este relatório seja aceito como base comum para o entendimento, seus conceitos e termos deveriam, de alguma forma, ser incorporados aos currículos universitários.

Por meio dessa fundamentação para o entendimento mútuo, todos os agentes poderão utilizar uma linguagem comum e comunicar-se, dessa forma, com maior eficácia. Os executivos de negócios terão condições de avaliar o processo de gestão de riscos corporativos de suas próprias organizações em relação a um padrão, fortalecer o processo e conduzir a organização rumo às metas estabelecidas. A pesquisa futura poderá, então, ser alavancada a partir de uma base existente. Os legisladores e os agentes reguladores também poderão adquirir um maior entendimento do gerenciamento de riscos corporativos, inclusive os seus benefícios e suas limitações. Se todos utilizarem uma estrutura comum de gestão de riscos corporativos, esses benefícios concretizar-se-ão.

COSO

Gerenciamento de Riscos Corporativos - Estrutura Integrada

Estrutura

1. Definição

Resumo do capítulo: Todas as organizações enfrentam incertezas, e o desafio de sua administração é determinar o nível de incerteza que a organização está preparada para aceitar, na medida em que se empenha em agregar valor para as partes interessadas. O gerenciamento de riscos corporativos não apenas permite identificar, avaliar e administrar riscos diante de incertezas, como também integra o processo de criação e preservação de valor. O gerenciamento de riscos corporativos é um processo conduzido pelo conselho de administração, pela diretoria executiva e pelos demais empregados, e aplicado no estabelecimento de estratégias por meio de toda a organização. Além de ser capaz de identificar eventos em potencial, capazes de afetar a organização, o processo permite o gerenciamento de riscos de forma compatível com o apetite a risco da organização e, ainda, possibilita um nível razoável de garantia em relação à realização dos seus objetivos. O processo é constituído de oito componentes inter-relacionados e integram o modo pelo qual a administração gerencia a organização. Os componentes são associados e servem de critério para determinar se o gerenciamento de riscos é eficaz ou não.

Um dos objetivos fundamentais dessa estrutura é contribuir para que a gestão de empresas e demais organizações adotem uma forma mais adequada de abordar os riscos inerentes ao cumprimento de seus objetivos. Entretanto, o significado de gestão de riscos corporativos varia de pessoa para pessoa e o processo recebe diversos rótulos e significados, o que constitue em obstáculo ao entendimento comum. Assim, uma meta importante seria integrar diversos conceitos de administração de riscos em uma única estrutura para a qual se estabelece uma definição comum, seus componentes são identificados e os conceitos fundamentais são descritos. Essa estrutura seria capaz de acomodar a maior parte das opiniões e, assim, possibilitar um ponto de partida na avaliação e no aprimoramento da gestão de riscos corporativos para futuras iniciativas de órgãos reguladores e de ensino.

Incerteza e Valor

Uma premissa subentendida do gerenciamento de riscos é que toda organização, seja ela com ou sem fins lucrativos ou órgão de governo, existe para gerar valor para as partes interessadas. Todas as organizações enfrentam incertezas, e o desafio da direção é determinar o nível de incerteza que ela está preparada para enfrentar na medida em que se empenha para aumentar o valor para as partes interessadas. As incertezas geram riscos e oportunidades, com potencial para destruir ou gerar valor. O gerenciamento de riscos corporativos possibilita aos administradores tratar com eficácia as incertezas, os riscos e as oportunidades a elas associados de forma a aprimorar a capacidade de geração de valor.

As organizações atuam em ambientes nos quais fatores como globalização, tecnologia, reestruturação, mercados em fase de transição, concorrência e regulamentos geram incerteza. A incerteza emana da incapacidade de se determinar com precisão a probabilidade de ocorrência de determinados eventos e impactos a eles associados. A incerteza também é apresentada e criada pelas escolhas estratégicas da organização. Por exemplo, uma organização possui uma estratégia de crescimento baseada na expansão de suas operações em outro país. Essa estratégia implica riscos e oportunidades associados à estabilidade do ambiente político do país, como recursos, mercados, canais, capacidade da força de trabalho e custos.

O valor é gerado, conservado ou destruído pelas decisões gerenciais em todas as atividades, da fixação de estratégias à operação cotidiana da organização. A criação de valor ocorre pela exploração de recursos, como pessoal, capital, tecnologia e marca, sendo o benefício obtido maior do que os recursos utilizados. A preservação do valor ocorre quando o valor gerado é sustentado por meio de, entre outras coisas, qualidade superior de produto, capacidade de produção e satisfação do cliente. O valor poderá desgastar-se, caso essas metas não sejam alcançadas por causa das deficiências na estratégia ou na sua execução. O reconhecimento dos riscos e das oportunidades, um fator inerente no processo decisório, requer que a administração analise as informações em relação aos ambientes interno e externo, utilize seus recursos, bem como ajuste as atividades às mudanças das circunstâncias.

O valor é maximizado quando a administração estabelece a estratégia e os objetivos a fim de alcançar um ponto de equilíbrio ideal entre as metas de crescimento e de retorno, bem como dos riscos a elas relacionados, além de explorar os recursos com eficiência e eficácia para atingir os objetivos da organização. O gerenciamento de riscos corporativos requer:

- Alinhar o apetite a risco e a estratégia – A administração considera em primeiro lugar o apetite a risco, ao avaliar as opções estratégicas e fixar objetivos compatíveis com a estratégia escolhida, bem como desenvolver mecanismos para administrar os riscos implícitos. Por exemplo, uma companhia farmacêutica apresenta reduzido apetite a risco em relação ao valor de sua marca. Da mesma forma, para proteger a sua marca, essa companhia adota amplos protocolos para garantir a segurança de seus produtos e realiza regularmente investimentos substanciais em pesquisa e desenvolvimento antecipados para dar suporte à criação de valor de marca.

- Otimizar as decisões de resposta a risco – O gerenciamento de riscos da organização fornece o rigor para identificar e escolher respostas alternativas aos riscos – prevenção, redução, compartilhamento e aceitação de riscos. Por exemplo, a administração de uma companhia, que opera uma frota particular, reconhece os riscos inerentes ao processo de entrega, incluindo custos de danos aos veículos e pessoais. As opções disponíveis contemplam reduzir os riscos por meio de um programa eficaz de recrutamento e treinamento de motoristas,

rejeitar os riscos terceirizando a entrega, compartilhar o risco por meio de seguro ou, simplesmente, aceitar o risco. O gerenciamento de riscos corporativos oferece metodologias e técnicas para a tomada dessas decisões.

- Reduzir surpresas e prejuízos operacionais – As organizações aprimoram sua capacidade de identificar eventos em potencial, avaliar os riscos e estabelecer respostas, reduzindo, assim, a probabilidade de surpresas e dos custos ou prejuízos inerentes a elas. Por exemplo, uma companhia monitora os índices de defeitos em peças e equipamentos da produção além dos desvios em relação às médias. A companhia avalia o impacto desses defeitos por diversos critérios, entre eles, o tempo necessário para o reparo, a incapacidade de atender à demanda do cliente, a segurança de empregados, o custo de reparos programados e imprevistos, e reage a esses prejuízos estabelecendo programações de manutenção.

- Identificar e administrar os riscos inerentes aos empreendimentos – Toda organização enfrenta uma série de riscos que afetam suas diferentes áreas. À administração cabe não apenas gerir os riscos individuais, mas também entender os impactos inter relacionados. Por exemplo, um banco enfrenta uma variedade de riscos ao executar suas transações que pode afetar toda a organização. Por esse motivo, a administração desenvolveu um sistema de informações que analisa dados de transações e de mercado de outros sistemas internos, os quais, aliados às informações relevantes geradas externamente, possibilitam uma visão conjunta dos riscos por meio de todas as atividades bancárias, O sistema de informações permite um enfoque detalhado no âmbito de departamento, cliente ou contraparte, operador e transação, além de quantificar o risco relativo às tolerâncias a risco em categorias estabelecidas. O sistema permite que o banco combine dados previamente discrepantes para responder aos riscos de forma eficaz, utilizando uma visão consolidada ou uma visão por objetivo.

- Fornecer respostas integradas aos diversos riscos – o ambiente de negócios traz em seu bojo inúmeros riscos inerentes. Por esse motivo, o gerenciamento de riscos corporativos possibilita soluções integradas para sua gestão. Por exemplo, um distribuidor atacadista enfrenta os riscos de estoques de suprimento em excesso ou em falta, fornecedores frágeis e preços de compra elevados, sem justificativa aparente. O gerenciamento identificou e avaliou os riscos no contexto da estratégia, os objetivos e as respostas alternativas da Companhia, e desenvolveu um sistema de controle de estoque de longo espectro. O sistema é integrado aos fornecedores e compartilha informações de vendas e de estoques, possibilitando uma parceria estratégica e evitando faltas de estoque e custos de carregamento, por meio de contratos de fornecimento para prazos mais dilatados e com melhores preços. Os fornecedores assumem a responsabilidade de reabastecer os estoques, gerando, assim, reduções adicionais de custos.

- Aproveitar as oportunidades – ao considerar toda uma série de eventos em potencial, em vez de apenas os riscos, a administração é capaz de identificar os eventos que representam oportunidades. Por exemplo, uma Companhia de alimentos, analisou potenciais eventos que provavelmente afetariam seu objetivo de crescimento sustentável de receita. Ao avaliá-los, a direção constatou que seus consumidores cativos demonstravam uma preocupação cada vez maior com a saúde e estavam modificando suas preferências alimentares, o que sinalizava um declínio na demanda futura dos produtos atuais. Para definir uma resposta, a administração identificou algumas formas de aplicação de seus atributos para desenvolver novos produtos, o que lhe permitiu preservar sua receita de clientes existentes e também, gerar receita adicional ao atrair uma base mais ampla de consumidores.

- Melhorar a alocação de capital – a obtenção de informações relevantes quanto aos riscos permite que a administração avalie as necessidades gerais de capital com maior eficiência e otimize a sua alocação. Por exemplo, uma instituição financeira passa a se sujeitar a novas normas regulamentares que aumentariam seus requisitos de capital, a menos que a administração calculasse os níveis de risco de crédito e operacional e as respectivas necessidades de capital com mais especificidade. A companhia avaliou o risco em termos de custo de desenvolvimento de sistema, relativamente aos custos adicionais de capital, e tomou uma decisão sobre essas informações. Mediante um software já existente e facilmente adaptável, a instituição desenvolveu cálculos mais precisos e evitou a necessidade de obter capital adicional.

Essas funcionalidades são inerentes à gestão de riscos corporativos, fato que ajuda a administração a alcançar as metas de desempenho e de rentabilidade da organização e a evitar a perda de recursos. O gerenciamento de riscos corporativos contribui para assegurar uma comunicação eficaz e para garantir que a organização está em conformidade com leis e regulamentos, o que evita danos à sua reputação e as conseqüências associadas. Em suma, o gerenciamento de riscos corporativos ajuda a organização a concretizar seus objetivos e evitar armadilhas e acontecimentos indesejáveis ao longo do exercício de suas atividades.

Eventos – Riscos e Oportunidades

Um evento é um incidente ou uma ocorrência gerada com base em fontes internas ou externas, que afeta a realização dos objetivos. Os eventos podem causar impacto negativo, positivo ou ambos. Os eventos que geram impacto negativo representam riscos. Da mesma forma, o risco é definido como segue:

> O risco é representado pela possibilidade de que um evento ocorrerá e afetará negativamente a realização dos objetivos.

Os eventos que causam impacto desfavorável são obstáculos à criação de valor ou desgastam o valor existente. Os exemplos incluem paradas no maquinário da fábrica, incêndio e perdas de créditos. Os eventos de impacto negativo podem originar-se a partir de condições aparentemente positivas, como nos casos em que a demanda de produto pelo consumidor é superior à capacidade de produção, o que provoca o não atendimento da demanda, o desgaste na fidelidade do cliente e o declínio de pedidos futuros.

Os eventos cujo impacto é positivo podem contrabalançar os impactos negativos ou representar oportunidades. A oportunidade é definida da seguinte forma:

> Oportunidade é a possibilidade de que um evento ocorra e influencie favoravelmente a realização dos objetivos.

As oportunidades favorecem a criação ou a preservação de valor. A direção da organização canaliza as oportunidades para seus processos de fixação de estratégias ou objetivos, formulando planos que visam ao seu aproveitamento.

Definição de Gerenciamento de Riscos Corporativos

O gerenciamento de riscos corporativos diz respeito aos riscos e às oportunidades de criar ou preservar valor, e é definido da seguinte forma:

> O gerenciamento de riscos corporativos é o processo conduzido em uma organização pelo Conselho de Administração, pela diretoria executiva e pelos demais funcionários, aplicado no estabelecimento de estratégias formuladas para identificar, em toda a organização, eventos em potencial, capazes de afetar a referida organização, e administrar os riscos para mantê-los compatíveis com o seu apetite a risco e possibilitar garantia razoável de cumprimento dos objetivos da entidade.

A definição a seguir reflete certos conceitos fundamentais. O gerenciamento de riscos corporativos é:

- um processo contínuo e que flui pela organização;
- conduzido pelos profissionais em todos os níveis da organização;
- aplicado à definição das estratégias;
- aplicado em toda a organização, em todos os níveis e unidades, e inclui a formação de uma visão de portfólio de todos os riscos a que ela está exposta;
- formulado de modo que identifique eventos em potencial, cuja ocorrência poderá afetar a organização, e que administre os riscos de acordo com o seu apetite a risco;
- capaz de propiciar garantia razoável para a diretoria executiva e para o conselho de administração de uma organização;
- orientado para à realização de objetivos em uma ou mais categorias distintas, mas dependentes.

Essa definição é intencionalmente ampla pelo fato de empregar conceitos fundamentais sobre a forma pela qual as empresas e outras organizações administram riscos, possibilitando uma base para a sua aplicação em diversos tipos de organização, indústria ou setor. O gerenciamento de riscos corporativos orienta seu enfoque diretamente para o cumprimento dos objetivos estabelecidos por uma entidade em particular. Fornece uma base para definir a eficácia do gerenciamento de riscos em uma organização, discutida posteriormente neste capítulo. Os conceitos fundamentais esboçados anteriormente são discutidos nos próximos parágrafos.

Um Processo

O gerenciamento de riscos corporativos não é estático; mais precisamente é uma ação contínua e interativa que permeia toda uma organização. Essas ações são difusas e inerentes à forma que a administração gerencia.

A perspectiva de alguns observadores sobre o gerenciamento de riscos é divergente, uma vez que este é considerado uma atividade adicional às já existentes na organização. Isso não quer dizer que uma gestão de riscos efetiva não possa erigir esforços adicionais, como realmente ocorre. Por exemplo, quando há riscos de crédito e de moeda, pode ser necessário um esforço adicional para desenvolver modelos, análises e cálculos complementares. Entretanto, esses mecanismos de gestão de riscos corporativos estão interligados às atividades operacionais da organização e existem por motivos comerciais básicos. O gerenciamento de riscos corporativos tem maior eficácia quando esses mecanismos são construídos como parte da infra-estrutura da organização e fazem parte de sua essência. Ao incorporar o gerenciamento de riscos corporativos em sua estrutura, uma organização será capaz de influenciar diretamente a habilidade de implementar suas estratégias e de realizar a sua missão.

A implantação do gerenciamento de riscos corporativos acarreta importantes implicações quanto à contenção de custos, especialmente nos mercados altamente competitivos que muitas organizações têm de enfrentar. A criação de novos procedimentos isolados daqueles existentes gera novos custos. Ao orientar seu enfoque para as operações existentes e na forma como estas podem contribuir para o gerenciamento de riscos corporativos e ao integrá-lo às atividades operacionais básicas, a organização poderá evitar procedimentos e custos desnecessários. Além disso, a prática de implantar e incorporar o gerenciamento de riscos corporativos à estrutura das operações contribui para que os responsáveis pela administração identifiquem e aproveitem novas oportunidades de crescimento dos negócios.

Conduzido por Pessoas

O gerenciamento de riscos corporativos é efetuado pelo conselho de administração, pela diretoria executiva e pelos demais empregados. É realizada pelas pessoas de uma organização, mediante o que fazem e o que dizem. São as pessoas que estabelecem a missão, a estratégia e os objetivos da organização e implementam os mecanismos de gerenciamento de riscos corporativos.

Da mesma forma, a gestão de riscos afeta as ações das pessoas, uma vez que reconhece que estas nem sempre entendem, se comunicam ou desempenham suas funções de forma consistente. Todo indivíduo traz para o local de trabalho não apenas um histórico, mas também habilidades técnicas singulares, além de possuir necessidades e prioridades diferentes.

Essas realidades intervêm e são influenciadas pelo gerenciamento de riscos corporativos. Cada pessoa possui um ponto único de referência que atua sobre o modo pelo qual essa pessoa identifica, avalia e responde a riscos. O gerenciamento de riscos corporativos proporciona os mecanismos necessários para ajudar as pessoas a entender o risco no contexto dos objetivos da organização. As pessoas devem conhecer suas responsabilidades e seus limites de autoridade. Do mesmo modo, deverá haver uma associação clara e estreita entre os deveres das pessoas e como elas os cumprem no tocante à estratégia e aos objetivos da organização.

Entre as pessoas que compõem uma organização estão o conselho de administração, a diretoria executiva e os demais empregados. A despeito do fato dos conselheiros da administração terem por função básica supervisionar, eles também direcionam e aprovam a estratégia e determinadas transações e políticas. Sendo assim, os conselhos da administração são um importante elemento para gerenciar os riscos corporativos.

Aplicado na Fixação da Estratégia

Uma organização não apenas define sua missão ou visão, mas também estabelece objetivos estratégicos, isto é, metas de alto nível que alinham e apóiam as decisões para o cumprimento destes. A organização estabelece uma estratégia para alcançar seus objetivos. Além disso, os objetivos relacionados que deseja alcançar, que, por meio da estratégia, fluirão em forma de cascata para suas unidades de negócios, divisões e processos.

O gerenciamento de riscos corporativos aplica-se ao processo de definir as estratégias, ocasião em que a administração leva em consideração os riscos relativos às diferentes alternativas. Por exemplo, uma delas poderá ser adquirir outras corporações visando um aumento da participação de mercado. A outra opção poderá ser um corte nos custos operacionais visando alcançar um porcentual mais elevado de margem bruta. Cada uma dessas alternativas traz vários riscos. Se a administração escolher a primeira estratégia, a Companhia poderá ter de estender as suas atividades a mercados novos e desconhecidos, os concorrentes talvez consigam aumentar sua participação nos seus mercados atuais, ou a companhia poderá deparar-se com a falta de capacidade para implementar efetivamente a estratégia. Com relação à segunda opção, os riscos incluem a necessidade de utilizar novas tecnologias ou fornecedores, ou de formar novas alianças. As técnicas de gestão de riscos são aplicadas nessa etapa para ajudar a administração a avaliar e a selecionar a estratégia e os objetivos a ela associados.

Aplicado em Toda a Organização

Ao aplicar o gerenciamento de riscos corporativos, deverá examinar as atividades em todos os níveis da organização, desde as atividades realizadas no âmbito empresarial, como planejamento estratégico e alocação de recursos, às atividades das unidades de negócios, como marketing e recursos humanos, e, ainda, analisar os processos do negócio, como produção e análise de crédito de clientes novos. O gerenciamento de riscos corporativos também se aplica a projetos especiais e a novas iniciativas que talvez não disponham de um local designado na hierarquia ou no organograma da organização.

O gerenciamento de riscos corporativos requer que a organização adote uma visão de portfólio dos riscos, procedimento que poderá exigir a participação de cada um dos gerentes responsáveis por unidades de negócios, funções, processos ou outras atividades que envolvam avaliação de risco, a qual poderá ser quantitativa ou qualitativa. Com uma visão combinada de cada nível da organização, a alta administração é capaz de avaliar se a carteira de riscos é compatível com o apetite a risco da organização.

A administração analisa a correlação entre os riscos a partir da perspectiva de portfólio no âmbito de toda a organização. Os riscos isolados a cada uma das suas unidades podem ser compatíveis com as tolerâncias a riscos dessas unidades, porém, tomados em conjunto, podem exceder o apetite a risco da organização como um todo. Ou, de modo contrário, os eventos em potencial podem representar riscos inaceitáveis para uma dada unidade de negócios, mas podem exercer um efeito compensador em outra. Os riscos inter-relacionados necessitam ser identificados e controlados, a fim de que a totalidade dos riscos seja compatível com o apetite a risco da organização.

Apetite a Risco

O apetite a risco é a quantidade de riscos, no sentido mais amplo, que uma organização está disposta a aceitar em sua busca para agregar valor. O apetite a risco reflete toda a filosofia administrativa de uma organização e, por sua vez, influencia a cultura e o estilo operacional desta. Muitas organizações consideram esse apetite de forma qualitativa, categorizando-o como elevado, moderado ou baixo, enquanto outras organizações adotam uma abordagem quantitativa que reflete e equilibra as metas de crescimento, retorno e risco. Uma organização dotada de um maior apetite a risco poderá desejar alocar grande parcela de seu capital para áreas de alto risco como mercados recém-emergentes. Por outro lado, uma organização com um reduzido apetite a risco poderá limitar seu risco de curto prazo investindo apenas em mercados maduros e mais estáveis.

O apetite a risco está diretamente relacionado à estratégia da organização e é levado em conta na ocasião de definir as estratégias, visto que a estas expõem a organização a diferentes riscos. O gerenciamento destes ajuda a administração a selecionar uma estratégia capaz de alinhar a criação de valor com o apetite a risco.

O apetite a risco orienta a alocação de recursos entre as unidades de negócios e as iniciativas, levando em consideração os riscos e o plano da unidade para gerar o retorno desejado dos recursos investidos. A administração considera o apetite a risco ao alinhar sua organização, seu pessoal e seus processos, e prepara a infra-estrutura necessária para responder e monitorar riscos com eficácia.

Associadas aos objetivos da organização, a tolerância a riscos representa o nível aceitável de variação em relação à meta para o cumprimento de um objetivo específico, e, via de regra, é mensurada nas mesmas unidades utilizadas para avaliar o objetivo a que está vinculada.

Ao estabelecer a tolerância a riscos, a administração considera o grau de importância do objetivo relacionado e alinha essas tolerâncias ao apetite a risco global. Tal operação ajuda a assegurar que a organização permaneça dentro de seus limites de apetite a risco e, por sua vez, consiga atingir os seus objetivos.

Possibilita Garantia Razoável

Um gerenciamento de riscos corporativos, formulado e executado adequadamente, será capaz de oferecer ao conselho de administração e à diretoria executiva garantia razoável do cumprimento de seus objetivos. A garantia razoável reflete a noção de que incertezas e riscos se relacionam com o futuro, o qual ninguém é capaz de prever com exatidão.

Essa garantia razoável não significa que o gerenciamento de riscos corporativos falhará com freqüência. Muitos fatores, individuais ou coletivos, reforçam o conceito de garantia razoável. O efeito cumulativo de respostas a riscos, que atendem a diversos objetivos, e o caráter multifuncional dos controles internos reduzem os riscos da organização não atingir seus objetivos. Além disso, as responsabilidades individuais e as atividades operacionais rotineiras, em vários níveis de uma organização, direcionarão o cumprimento de seus objetivos. Espera-se que, entre diversas organizações adequadamente controladas, a maioria seja periodicamente informada de seu progresso quanto ao cumprimento de seus objetivos estratégicos e operacionais, que estes sejam conquistados regularmente e que relatórios confiáveis sejam elaborados de forma consistente, período após período, ano após ano. Entretanto, poderá ocorrer um evento incontrolável, um erro, ou um incidente. Em outras palavras, até mesmo um gerenciamento de riscos corporativos eficaz poderá falhar. Garantia razoável não é garantia absoluta.

Cumprimento dos Objetivos

Com base na missão estabelecida, a administração planeja objetivos principais, seleciona as estratégias e estabelece outros planos a serem adotados por toda a organização, alinhados com a estratégia e a ela vinculados. Embora muitos objetivos sejam específicos a uma determinada organização, alguns deles são amplamente compartilhados. Por exemplo, os objetivos comuns a praticamente todas as entidades são alcançar e manter uma reputação favorável tanto no segmento empresarial quanto com seus clientes, fornecer informações confiáveis às partes interessadas e operar em conformidade com as leis e a regulamentação.

Essa estrutura estabelece quatro categorias de objetivos para a organização:

- Estratégicos – referem-se às metas no nível mais elevado. Alinham-se e fornecem apoio à missão.
- Operações – têm como meta a utilização eficaz e eficiente dos recursos.
- Comunicação – relacionados à confiabilidade dos relatórios.
- Conformidade – fundamentam-se no cumprimento das leis e dos regulamentos pertinentes.

Essa classificação possibilita um enfoque nos aspectos específicos do gerenciamento de riscos corporativos. Apesar de essas categorias serem distintas, elas se inter-relacionam, uma vez que um dado objetivo poderá estar presente em mais de uma categoria, elas tratam de necessidades empresariais diferentes, cuja responsabilidade direta poderá ser atribuída a diversos executivos. Essa classificação também possibilita distinguir o que se espera do gerenciamento de riscos corporativos.

Algumas organizações utilizam outra categoria de objetivos, “a salvaguarda de recursos”, que também é denominada “salvaguarda de ativos”. De modo geral, esses objetivos têm como meta evitar a perda de ativos ou recursos da organização, seja por meio de furto, desperdício, ineficiência, ou simplesmente, por meio de decisões empresariais equivocadas, como vender um produto a preço demasiado baixo, deixar de conservar empregados de importância fundamental, evitar infrações a patentes, ou incorrer em passivos imprevistos. Esses objetivos são essencialmente de natureza operacional, embora determinados aspectos de salvaguarda possam ser classificados em outras categorias. Nos casos da aplicação de exigências legais ou regulamentares, os referidos objetivos tornam-se itens de *compliance*. Quando considerados em conjunto com informações públicas, utiliza-se uma definição mais rigorosa para a salvaguarda de ativos. Essa definição trata da prevenção ou constatação oportuna, de aquisição, do uso ou da alienação não autorizada dos bens de uma organização, que poderia produzir impacto relevante nas demonstrações financeiras.

Espera-se que o gerenciamento de riscos corporativos ofereça garantia razoável do cumprimento dos objetivos relacionados à confiabilidade dos informes e ao cumprimento de leis e regulamentos. O atendimento dessas categorias de objetivos está sob o controle da organização e depende da qualidade da execução das atividades a elas relacionadas.

Entretanto, o alcance de objetivos estratégicos, como, por exemplo, a conquista de uma determinada participação de mercado, e de objetivos operacionais, como o lançamento bem-sucedido de uma nova linha de produtos, nem sempre está sob total controle da organização. O gerenciamento de riscos corporativos não consegue neutralizar julgamentos ou decisões equivocadas, nem eventos externos, responsáveis por levar um negócio a deixar de alcançar suas metas operacionais. No entanto, esse gerenciamento é capaz de aumentar a probabilidade da administração tomar decisões melhor fundamentadas. Em relação a esses objetivos, o gerenciamento de riscos corporativos pode oferecer garantia razoável para que a diretoria executiva e o conselho de administração, na função de supervisores, sejam oportunamente notificados se a organização está na direção do cumprimento dos objetivos.

Componentes do gerenciamento de riscos corporativos

O gerenciamento de riscos corporativos é constituído de oito componentes inter-relacionados, que se originam com base na maneira como a administração gerencia a organização, e que se integram ao processo de gestão. Esses componentes são os seguintes:

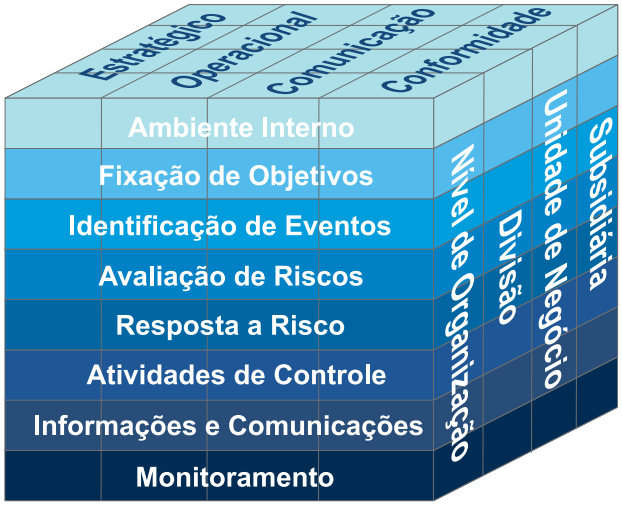
- Ambiente Interno – A administração estabelece uma filosofia quanto ao tratamento de riscos e estabelece um limite de apetite a risco. O ambiente interno determina os conceitos básicos sobre a forma como os riscos e os controles serão vistos e abordados pelos empregados da organização. O coração de toda organização fundamenta-se em seu corpo de empregados, isto é, nos atributos individuais, inclusive a integridade, os valores éticos e a competência – e, também, no ambiente em que atuam.
- Fixação de Objetivos – Os objetivos devem existir antes que a administração identifique as situações em potencial que poderão afetar a realização destes. O gerenciamento de riscos corporativos assegura que a administração adote um processo para estabelecer objetivos e que os escolhidos propiciem suporte, alinhem-se com a missão da organização e sejam compatíveis com o apetite a risco.
- Identificação de Eventos – Os eventos em potencial que podem impactar a organização devem ser identificados, uma vez que esses possíveis eventos, gerados por fontes internas ou externas, afetam a realização dos objetivos. Durante o processo de identificação de eventos, estes poderão ser diferenciados em riscos, oportunidades, ou ambos. As oportunidades são canalizadas à alta administração, que definirá as estratégias ou os objetivos.
- Avaliação de Riscos – Os riscos identificados são analisados com a finalidade de determinar a forma como serão administrados e, depois, serão associados aos objetivos que podem influenciar. Avaliam-se os riscos considerando seus efeitos inerentes e residuais, bem como sua probabilidade e seu impacto.
- Resposta a Risco – Os empregados identificam e avaliam as possíveis respostas aos riscos: evitar, aceitar, reduzir ou compartilhar. A administração seleciona o conjunto de ações destinadas a alinhar os riscos às respectivas tolerâncias e ao apetite a risco.
- Atividades de Controle – Políticas e procedimentos são estabelecidos e implementados para assegurar que as respostas aos riscos selecionados pela administração sejam executadas com eficácia.
- Informações e Comunicações – A forma e o prazo em que as informações relevantes são identificadas, colhidas e comunicadas permitam 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.
- Monitoramento – A integridade do processo de gerenciamento de riscos corporativos é monitorada e as modificações necessárias são realizadas. Desse modo, a organização poderá reagir ativamente e mudar segundo as circunstâncias. O monitoramento é realizado por meio de atividades gerenciais contínuas, avaliações independentes ou uma combinação desses dois procedimentos.

O gerenciamento de riscos corporativos é um processo dinâmico. Por exemplo, a avaliação de riscos não apenas dará origem a uma resposta aos riscos, mas também poderá influenciar as atividades de controle e destacar o fato de reconsiderar tanto as necessidades de informação e de comunicação da organização ou quanto as suas atividades de monitoramento. Desse modo, o gerenciamento de riscos corporativos não é um processo rigorosamente em série, pelo qual um componente afeta apenas o seguinte; é um processo multidirecional e interativo, segundo o qual quase todos os componentes podem e realmente influenciam os demais.

É praticamente impossível que duas organizações venham ou devam aplicar o gerenciamento de riscos de uma forma idêntica. As organizações e suas características e necessidades de administração de riscos diferem amplamente de acordo com o setor e o porte, e segundo a filosofia e cultura administrativa. Desse modo, embora todas as organizações devam ter cada um dos componentes implementados e funcionando efetivamente, a aplicação do gerenciamento de riscos corporativos, inclusive com o emprego de ferramentas e técnicas e a atribuição de funções e responsabilidades, geralmente serão muito específicas.

Relacionamento entre Objetivos e Componentes

Existe um relacionamento direto entre os objetivos que uma organização se empenha em alcançar e os componentes do gerenciamento de riscos corporativos, que representam aquilo que é necessário para o seu alcance. Esse relacionamento é apresentado a seguir por meio de uma matriz tridimensional, em forma de cubo, apresentada no Anexo 1.1:



Anexo 1.1

- As quatro categorias de objetivos - estratégicos, operacionais, de comunicação e conformidade - estão representadas nas colunas verticais.
- Os oito componentes, nas linhas horizontais.
- A organização e as unidades de uma organização, na terceira dimensão do cubo.

A linha de cada componente “atravessa” e se aplica a todas as quatro categorias de objetivos. Por exemplo, os dados financeiros e não financeiros gerados a partir de fontes internas e externas, pertencentes ao componente de informação e comunicação, são necessários para estabelecer a estratégia, administrar as operações comerciais com eficácia, comunicar com eficácia e certificar-se de que a organização esteja cumprindo as leis aplicáveis.

Da mesma forma, se observarmos as categorias de objetivos, todos os oito componentes são relevantes entre si. Se tomarmos a categoria eficácia e eficiência das operações, por exemplo, todos os oito componentes inter-relacionam-se e são importantes para sua realização.

O gerenciamento de riscos corporativos é relevante a toda a organização ou a qualquer uma de suas unidades. Esse relacionamento é ilustrado pela terceira dimensão, que representa subsidiárias, divisões e outras unidades de negócios. Conseqüentemente, é possível concentrar-se em qualquer uma das células dessa matriz. Por exemplo, poderíamos considerar que a célula superior posterior direita represente o ambiente interno, visto estar relacionada com os objetivos de *compliance* de uma dada subsidiária.

Deve-se reconhecer que as quatro colunas representam categorias de objetivos de uma organização e não partes das unidades desta. Conseqüentemente, ao considerarmos a categoria de objetivos relacionados à comunicação, por exemplo, será necessário conhecer uma ampla gama de informações referentes às operações da organização.

Eficácia

Embora o gerenciamento de riscos corporativos seja um processo, a sua eficácia é um estado ou uma condição em um ponto no tempo. Podemos determinar a eficácia do gerenciamento de riscos corporativos de uma organização mediante um julgamento com base na presença e no bom funcionamento dos oito componentes. Assim sendo, os componentes também são critérios para um gerenciamento de riscos corporativos eficaz. Para que os componentes possam estar presentes e funcionar adequadamente, não poderá apresentar uma fraqueza significante, e as necessidades de riscos devem ser trazidas para dentro da faixa de apetite a risco da organização. Quando se determina que o gerenciamento de riscos corporativos é eficaz em cada uma das quatro categorias de objetivos, respectivamente, a diretoria executiva e o conselho de administração terão garantia razoável que:

- entendem até que ponto os objetivos estratégicos estão sendo alcançados;
- entendem até que ponto os objetivos operacionais estão sendo alcançados;
- a comunicação por relatórios é confiável;
- as leis e os regulamentos cabíveis estão sendo observados.

A despeito do fato de que todos os oito componentes devem estar presentes e funcionando adequadamente para que o gerenciamento de riscos corporativos possa ser considerado eficaz – aplicando-se os princípios descritos nos próximos capítulos – poderá haver algum desequilíbrio entre os componentes. Como as técnicas de gestão de riscos corporativos podem ser aplicadas com diversos propósitos, poderão estar presentes em mais de um componente. Além disso, as respostas a risco podem diferir quanto ao efeito sobre um determinado risco. Controles e respostas a risco complementares, que isoladamente apresentam efeito limitado, podem ter efeito conjunto satisfatório.

Os conceitos ora discutidos aplicam-se a todas as organizações independentemente do tamanho. Embora algumas organizações de pequeno e médio portes possam implementar os componentes de forma diferente das organizações de grande porte, estas ainda poderão desfrutar de um gerenciamento de riscos corporativos eficaz. A metodologia para cada componente será provavelmente menos formal e menos estruturada em pequenas organizações do que nas maiores, porém os conceitos básicos devem estar presentes em todas as organizações.

Via de regra; o gerenciamento de riscos corporativos é considerado, no contexto da organização, como um todo; o que implica considerar a sua aplicação em unidades de negócios relevantes. Entretanto, poderá haver circunstâncias nas quais a eficácia do gerenciamento de riscos corporativos deva ser avaliada separadamente em relação a uma determinada unidade de negócios. Nessas circunstâncias, para que se possa concluir a eficácia do gerenciamento de riscos corporativos dessa unidade todos os oito componentes devem estar presentes e funcionando bem na própria unidade. Assim, por exemplo, o fato de haver um conselho de administração com atribuições específicas como parte do ambiente interno, o gerenciamento de riscos corporativos para uma determinada unidade de negócios pode apenas ser considerada eficaz, se tiver implementado seu próprio conselho ou um órgão semelhante (ou o conselho de administração da entidade supervisiona diretamente a unidade de negócios). Da mesma forma, em razão do componente de resposta a risco estipular que se deve adotar uma visão de portfólio dos riscos, para que o gerenciamento de riscos corporativos possa ser efetivamente avaliado, a organização deverá apresentar uma visão de portfólio dos riscos da referida unidade de negócios.

Abrangência do Controle Interno

O controle interno é parte integrante do gerenciamento de riscos corporativos. A referida estrutura de gestão de riscos corporativos abrange o controle interno; originando uma conceituação e uma ferramenta de gestão mais robusta. O controle interno é definido e descrito em “Controle Interno – Estrutura Integrada”. Tendo em vista que o “Controle Interno – Estrutura Integrada” tenha resistido ao tempo e sido a base das normas existentes, dos regulamentos e das leis, o documento permanece vigente como fonte de definição e marco para as estruturas de controle interno. Embora apenas algumas partes do texto de “Controle Interno – Estrutura Integrada” tenham sido reproduzidas na presente estrutura, a totalidade do “Controle Interno – Estrutura Integrada” está incorporada como referência. O “Apêndice C” descreve a relação entre gestão de riscos corporativos e controle interno.

Gerenciamento de riscos corporativos e o Processo de Gestão

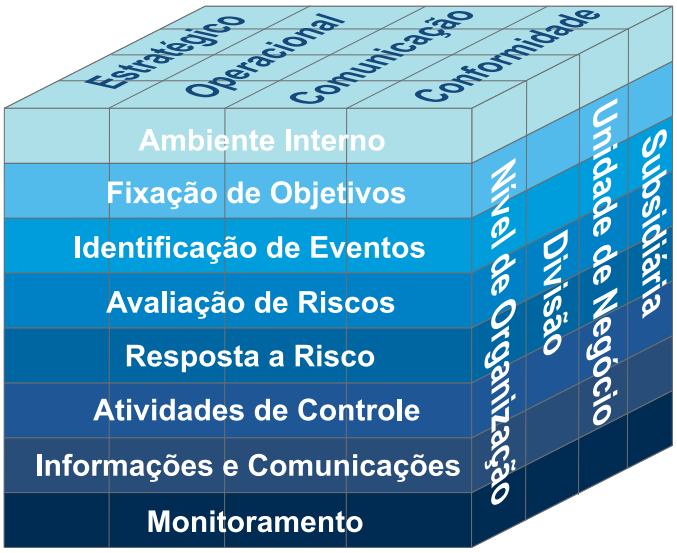
Em razão do gerenciamento de riscos corporativos ser uma das atividades de todo o processo de gestão, os componentes dessa estrutura são discutidos no contexto das ações da direção ao administrar uma unidade negócio ou toda uma organização. Porém, nem todas as atividades da administração fazem parte do gerenciamento de riscos corporativos. Muitas das opiniões e dos julgamentos aplicados no processo decisório de uma administração, bem como as ações gerenciais decorrentes, embora parte do processo de gestão, não fazem parte do processo de gestão de riscos corporativos. Por exemplo:

- O procedimento que assegura a existência de um processo apropriado para a fixação de objetivos é um componente crítico do gerenciamento de riscos corporativos, porém os objetivos específicos selecionados pela administração não fazem parte desse gerenciamento.
- Responder aos riscos, tendo-se por base uma avaliação adequada desses, faz parte do gerenciamento de riscos corporativos, porém as respostas específicas selecionadas e a respectiva alocação dos da empresa não o integram nesse gerenciamento.
- Estabelecer e executar atividades de controle para assegurar que as respostas aos riscos, que a administração venha a escolher, sejam realizadas com eficácia, faz parte do gerenciamento de riscos corporativos, porém as atividades específicas de controle não o integram.

De um modo geral, o gerenciamento de riscos corporativos abrange os elementos do processo administrativo que possibilitam à administração tomar decisões de risco bem informadas, porém as decisões específicas selecionadas, a partir de uma série de escolhas possíveis, não são capazes de determinar se o gerenciamento de riscos corporativos está sendo eficaz. Contudo, embora os objetivos específicos, as respostas aos riscos e as atividades de controle selecionadas sejam uma questão de julgamento administrativo, as escolhas devem possibilitar a redução dos riscos a um nível aceitável, conforme determinados pelo apetite a risco e a garantia razoável em relação à realização dos objetivos da organização.

2. Ambiente Interno

Resumo do Capítulo: O ambiente interno abrange a cultura de uma organização, a influência sobre a consciência de risco de seu pessoal, sendo a base para todos os outros componentes do gerenciamento de riscos corporativos, possibilita disciplina e a estrutura. Os fatores do ambiente interno compreendem a filosofia administrativa de uma organização no que diz respeito aos riscos; o seu apetite a risco; a supervisão do conselho de administração; a integridade, os valores éticos e a competência do pessoal da organização; e a forma pela qual a administração atribui alçadas e responsabilidades, bem como organiza e desenvolve o seu pessoal.



O ambiente interno é a base para todos os outros componentes do gerenciamento de riscos corporativos, o que propicia disciplina e estrutura. Esse ambiente influencia o modo pelo qual as estratégias e os objetivos são estabelecidos, os negócios são estruturados, e os riscos são identificados, avaliados e geridos. Este influencia o desenho e o funcionamento das atividades de controle, dos sistemas de informação e comunicação, bem como das atividades de monitoramento.

Sendo influenciado pela história e cultura de uma organização, o ambiente interno compreende muitos elementos, inclusive os valores éticos da organização, a competência e o desenvolvimento de pessoal, a filosofia da administração para a gestão de riscos, e como são atribuídas alçada e responsabilidade. O conselho de administração é parte crítica do ambiente interno e influencia muito os demais elementos de ambiente interno.

Embora todos os elementos sejam importantes, o grau de tratamento de cada um deles variará de acordo com a organização. Por exemplo, o presidente-executivo de uma corporação, dotada de uma pequena força de trabalho e de operações centralizadas, poderá não estabelecer linhas formais de responsabilidade ou políticas operacionais detalhadas. Entretanto, a Companhia pode dispor de um ambiente interno capaz de possibilitar uma base adequada para o gerenciamento de riscos corporativos.

Filosofia de Gestão de Riscos

A filosofia de gestão de riscos de uma organização é representada pelo conjunto de convicções e atitudes compartilhadas que caracterizam a forma pela qual a referida organização considera o risco em tudo aquilo que faz, do desenvolvimento e da implementação de estratégias às suas atividades do dia-a-dia. Sua filosofia de administração de riscos reflete em seus valores, influencia a sua cultura e seu estilo de operação, bem como afeta a forma que os componentes de gestão de riscos são aplicados inclusive como os riscos são identificados, os tipos de riscos aceitáveis e a forma pela qual são administrados.

Uma organização que tenha sido bem-sucedida em aceitar riscos significativos provavelmente terá uma visão diferente de gestão de riscos do que aquela que tenha enfrentado conseqüências severas, econômicas ou legais, como resultado de sua aventura em território perigoso. Embora algumas organizações busquem alcançar um gerenciamento de riscos corporativos eficaz para atender aos requerimentos de uma parte externa interessada, como a sua controladora ou o órgão regulador, a administração, freqüentemente, reconhece que a gestão de riscos corporativos eficaz contribuirá para criação ou preservação de valor da organização.

Quando a filosofia de administração de riscos está adequadamente desenvolvida, entendida e aceita pelo pessoal da organização, ela estará em condições de identificar e administrar riscos com eficácia. De outra forma, poderá ocorrer uma aplicação inaceitável e irregular do gerenciamento de riscos corporativos por meio das unidades de negócios ou departamentos. Porém, mesmo que a filosofia de uma organização encontre-se adequadamente desenvolvida, poderá existir diferenças culturais entre as suas unidades, o que provocará uma variação na aplicação do gerenciamento de riscos corporativos. Gestores de determinadas unidades podem mostrar-se preparados para enfrentar mais risco, enquanto outros assumem posições mais conservadoras. Por exemplo, uma função agressiva de vendas poderá orientar um esforço para a realização de vendas, sem dedicar a atenção devida a questões de cumprimento de normas, enquanto a unidade de contratação de pessoal dedica muita atenção ao cumprimento de políticas e regulamentos internos e externos pertinentes. Atuando isoladamente, essas diferentes subculturas poderiam afetar desfavoravelmente a organização. Porém, ao trabalharem em conjunto, as unidades poderão refletir adequadamente na filosofia de administração de riscos.

A filosofia de administração de riscos está virtualmente refletida em tudo aquilo que a administração faz para gerir a organização. Essa filosofia é apresentada em declarações a respeito das políticas, comunicações verbais e escritas, bem como durante o processo decisório. Quer a administração enfatize políticas, normas de conduta, indicadores de desempenho e relatórios de exceções, quer opere mais informalmente, principalmente mediante contato pessoal com gerentes-chave, é de importância crítica que a administração reforce a filosofia não apenas com palavras, mas também por meio de ações do cotidiano.

Apetite a risco

O apetite a risco refere-se ao nível de riscos, que de forma ampla, uma organização dispõe-se a aceitar na busca de valor. O apetite a risco reflete na filosofia de gestão de riscos corporativos e, por sua vez, influencia a cultura e o estilo de operação.

O apetite a risco é considerado no estabelecimento da estratégia, quando o retorno desejado de uma estratégia deve estar alinhado ao apetite a risco da organização. Diferentes estratégias exporão a organização a diferentes níveis de riscos, e o gerenciamento de riscos corporativos aplicado à fixação da estratégia ajuda a administração a optar pela solução que seja consistente com o apetite a risco.

As organizações consideram o apetite a risco de forma qualitativa, classificando-o em categorias como elevado, moderado ou baixo, ou adotam, ainda, uma abordagem quantitativa, que reflete e equilibra as metas de crescimento e retorno aos riscos.

Conselho de administração

O conselho de administração de uma organização representa uma parte crítica do ambiente interno e é capaz de influenciar os seus elementos de forma significativa. Cada fator, como a independência do conselho em relação à administração, à experiência e ao desenvolvimento de seus membros, o grau de participação e exame das atividades, bem como a adequação de suas ações, tem a sua importância. Outros fatores são, até que ponto questões complexas são levantadas e são abordadas com a diretoria executiva, no que se diz respeito a estratégia, planos, desempenho, bem como a interação que o conselho de administração ou comitê de auditoria possui com os auditores internos e externos.

Um conselho de administração ativo e empenhado, ou órgão similar, poderiam ter um grau adequado de conhecimento gerencial, técnico ou de outro tema específico com a disposição necessária para o desempenho de suas responsabilidades de supervisão. Esses fatores são críticos a um ambiente eficaz de gerenciamento de riscos corporativos. E, em razão dos membros do conselho estarem preparados para questionar e examinar as atividades da administração, apresentar opiniões alternativas e atuar em caso de gestão inadequada, conselho de administração deve incluir diretores-executivos de outras organizações.

Membros de diretorias executivas poderão tornar-se membros eficazes do conselho de administração, ao oferecer seus conhecimentos profundos em benefício da organização. Porém, deverá existir um número suficiente de membros externos e independentes, não apenas para propiciar orientação, aconselhamento e instruções adequados, como também para atuar com controle e equilíbrio necessários para a administração. Para que o ambiente interno seja eficaz, o conselho de administração deverá ser, no mínimo, composta em sua maioria por membros externos independentes.

Conselhos eficazes garantem que a administração mantenha um gerenciamento de riscos eficaz. A despeito do fato que, historicamente, uma organização não tenha incorrido em prejuízos e nem se exponha muito a riscos, os membros do conselho não devem sucumbir à noção mítica de que eventos que trazem sérias conseqüências adversas não “vão ocorrer aqui.” Eles reconhecem que, embora uma organização possa ter uma estratégia perfeita, empregados competentes, processos íntegros e tecnologia confiável, ela, como qualquer outra entidade, é vulnerável a risco e necessita de um processo de gestão de riscos eficaz.

Integridade e Valores Éticos

A estratégia e os objetivos de uma organização e o modo pelo qual são implementados baseiam-se em preferências, julgamentos de valor e estilos gerenciais. A integridade e o compromisso da administração com valores éticos influenciam essas preferências e esses julgamentos, os quais são traduzidos em normas de comportamento. A boa reputação de uma organização pode ser tão valiosa que os seus padrões de comportamento devem estender-se além do mero cumprimento de normas. Os gerentes de organizações bem administradas aceitam cada vez mais o conceito que a ética compensa e que o comportamento ético é um bom negócio.

A integridade da administração é um pré-requisito para o comportamento ético em todos os aspectos das atividades de uma organização. A eficácia do gerenciamento de riscos corporativos não deve estar acima da integridade e dos valores éticos das pessoas que criam, administram e monitoram as atividades da organização. Integridade e valores éticos são elementos essenciais ao ambiente interno das organizações, que influenciam o traçado, a administração e o monitoramento dos outros componentes do gerenciamento de riscos corporativos.

Via de regra, é difícil estabelecer valores éticos, dada a necessidade de levarem-se em conta os interesses de várias partes. Os valores administrativos devem equilibrar os interesses da organização, dos empregados, dos fornecedores, dos clientes, dos concorrentes e do público em geral. Tentar equilibrar esses interesses pode revelar-se uma tarefa complexa e frustrante por causa de freqüentes conflitos de interesses. Por exemplo, o fornecimento de um produto essencial (petróleo, madeira ou alimento) pode gerar preocupações ambientais.

O comportamento ético e a integridade administrativa são subprodutos da cultura corporativa, que compreende as normas éticas e comportamentais, e a forma pela qual elas são comunicadas e reforçadas. Políticas oficiais estipulam aquilo que o conselho e a administração desejam que aconteça. A cultura corporativa determina aquilo que efetivamente ocorre e quais normas serão observadas, distorcidas ou ignoradas. A alta administração – a começar pelo presidente – desempenha um papel fundamental na determinação da cultura corporativa. Visto que a personalidade dominante de uma organização, o presidente, geralmente estabelece a tonalidade ética.

Determinados fatores organizacionais também podem influenciar a probabilidade de práticas fraudulentas e questionáveis de *mascarar* as demonstrações financeiras. Esses mesmos fatores também podem influenciar o comportamento ético. Determinados indivíduos poderão cometer atos desonestos, ilegais ou antiéticos simplesmente porque a organização lhes propicia forte incentivo ou tentação para agir dessa forma. A ênfase injustificada em resultados, especialmente nos resultados de curto prazo, pode fomentar um ambiente interno inadequado. Um enfoque exclusivamente orientado aos resultados de curto prazo poderá ser prejudicial até mesmo ao curto prazo. Concentração exagerada no lucro – venda ou lucro a qualquer custo – freqüentemente evoca ações e reações imprevisíveis. Táticas agressivas de vendas, falta de consideração em negociações ou ofertas implícitas de suborno, por exemplo, podem suscitar reações de efeitos imediatos (bem como duradouros).

Outros incentivos para a utilização de práticas de relatórios fraudulentos ou questionáveis e, por extensão, outras modalidades de comportamento antiético podem incluir gratificações fortemente dependentes das demonstrações financeiras e não financeiras, especialmente no que se refere a resultados a curto prazo.

A remoção ou a redução de tentações e os incentivos inadequados são muito eficazes na eliminação do comportamento indesejável. Como já sugerimos, pode-se alcançar essa situação observando-se práticas comerciais íntegras e lucrativas. Por exemplo, os incentivos de desempenho – acompanhados dos controles apropriados – podem ser uma técnica valiosa de gestão, desde que as metas de desempenho sejam realistas. A fixação de metas realistas é uma prática motivacional sadia, capaz de reduzir o estresse contraproducente, e o incentivo à elaboração de relatórios fraudulentos. Do mesmo modo, um sistema de relatórios adequadamente controlado poderá servir de salvaguarda contra a tentação de mascarar o desempenho.

Outra causa de práticas duvidosas é a ignorância. Os valores éticos não devem ser apenas comunicados, mas acompanhados de orientação específica em relação ao certo e ao errado.

Os códigos formais de conduta corporativa também são importantes para o estabelecimento de um programa ético eficaz. Os códigos abordam uma variedade de questões comportamentais, como integridade e ética, conflitos de interesse, pagamentos ilegais ou inadequados e acordos anticompetitivos. Também são importantes os canais de comunicação ascendente nos quais os empregados sintam-se à vontade para veicular informações relevantes.

A existência de um código de conduta escrito, documentação que os empregados tenham recebido e entendido, e um canal adequado de comunicação não asseguram que o código seja observado. Também é importante prever penalidades para os empregados que infringem o código, mecanismos que incentivem o empregado a comunicar suspeitas de infrações, e medidas disciplinares contra os empregados que intencionalmente deixam de relatar infrações. Porém, o cumprimento das normas éticas, estejam ou não incorporadas em um código escrito, será tão ou mais garantido quando apoiado pelas ações e pelos exemplos da alta administração. É muito provável que os empregados desenvolvam as mesmas atitudes em relação ao certo e ao errado – e em relação a riscos e controles – como os mostrados pela alta administração. As mensagens mediante ações da diretoria executiva, rapidamente serão incorporadas na cultura corporativa. E o simples fato de que o Presidente tenha feito a coisa certa em termos de ética, quando confrontado com uma difícil decisão, envia uma mensagem poderosa por toda a organização.

Compromisso com a Competência

A competência reflete no conhecimento e nas habilidades necessárias à execução de tarefas designadas. A administração decide quão bem essas tarefas necessitam ser executadas, ponderando a estratégia e os objetivos da organização, bem como os planos para a sua implementação e realização. Freqüentemente haverá um dilema entre competência e custo – não é necessário, por exemplo, contratar um engenheiro para trocar uma lâmpada.

A administração estipula os níveis de competência para determinados trabalhos e traduz esses níveis em habilidades e conhecimentos necessários. As habilidades e os conhecimentos necessários, por sua vez, podem depender do grau de inteligência, treinamento e experiência individuais. Os fatores considerados no desenvolvimento dos níveis de conhecimentos e habilidades incluem a natureza e o grau de julgamento utilizado em uma função específica. Freqüentemente, pode-se efetuar uma troca entre a extensão da supervisão e os requisitos de competência do indivíduo.

Estrutura Organizacional

A estrutura organizacional de uma entidade provê o arcabouço para planejar, executar, controlar e monitorar as suas atividades. Uma estrutura organizacional relevante inclui a definição de áreas fundamentais de autoridade e responsabilidade, bem como a definição de linhas apropriadas de comunicação. Por exemplo, uma função de auditoria interna deve ser estruturada a fim de poder alcançar objetividade organizacional e permitir acesso irrestrito à alta administração e ao comitê de auditoria do conselho de administração, devendo o executivo chefe de auditoria reportar-se a um nível da organização que permita à atividade de auditoria interna cumprir com as suas responsabilidades.

As corporações desenvolvem estruturas organizacionais compatíveis com as suas necessidades. Algumas são centralizadas, outras descentralizadas; algumas apresentam reporte direto, enquanto que outras são matriciais. Determinadas organizações são estruturadas por ramo industrial ou linha de produto, localização geográfica ou por uma rede especial de distribuição ou de marketing. Outras organizações, inclusive muitas unidades governamentais municipais e estaduais e instituições sem fins lucrativos, são estruturadas por função.

A adequação da estrutura organizacional de uma entidade depende em parte de seu tamanho e da natureza de suas atividades. Uma organização altamente estruturada, com linhas formais de comunicação e responsabilidades, poderá ser adequada para uma organização de grande porte com numerosas divisões operacionais, inclusive operações no exterior. Porém, esse tipo de estrutura pode prejudicar o fluxo necessário de informações em uma organização de pequeno porte. Qualquer que seja a estrutura, a entidade deve estar organizada de modo a possibilitar um gerenciamento de riscos corporativos eficaz e desempenhar as suas atividades de modo a atingir os seus objetivos.

Atribuição de Alçada e Responsabilidade

A atribuição de alçada e responsabilidade inclui até que ponto pessoas e equipes estão autorizadas e são incentivadas a adotar sua própria iniciativa ao abordar questões, bem como a solucionar problemas e os limites dessa autoridade. Esse procedimento também inclui as relações de comunicação e protocolos de autorização, bem como as políticas que descrevem práticas apropriadas de negócios, conhecimento e experiência dos funcionários essenciais e os recursos fornecidos para cumprir as suas obrigações.

Algumas organizações deslocaram o nível de autoridade para baixo a fim de trazer o processo decisório ao pessoal da linha de frente. Uma Companhia poderá valer-se desse artifício para tornar-se mais orientada ao mercado e concentrada na qualidade – talvez para eliminar defeitos, reduzir o período do ciclo do negócio, ou aumentar a satisfação do cliente. O alinhamento da alçada e da responsabilidade é geralmente realizado para incentivar iniciativas individuais, dentro dos limites correspondentes. A delegação de autoridade significa passar o controle central de determinadas decisões aos escalões inferiores – para as pessoas que estão mais próximas das transações comerciais cotidianas. Isso pode envolver a delegação de poderes para vender produtos com desconto, negociar contratos de fornecimento, licenças, ou patentes em longo prazo, ou, ainda, ingressar em alianças ou empreendimentos conjuntos.

O desafio crucial é delegar apenas até o grau necessário ao alcance dos objetivos. Isso significa assegurar que o processo decisório esteja embasado em práticas sadias de identificação e avaliação de riscos, inclusive o dimensionamento de riscos e a comparação entre o potencial de prejuízo com os ganhos na determinação de quais riscos aceitar e de como serão administrados.

Outro desafio é assegurar que todo o pessoal entenda os objetivos da organização. É essencial que as pessoas entendam de que forma suas ações se inter-relacionam e contribuem para a realização dos objetivos.

Às vezes, o aumento da delegação é intencionalmente seguido da dinamização ou do “enxugamento” da estrutura organizacional. Uma mudança propositada para incentivar a criatividade, a iniciativa individual e os tempos de resposta mais curtos podem intensificar a competitividade e melhorar a satisfação do cliente. Esse aumento do grau de delegação pode trazer um requisito implícito de um nível mais elevado de competência dos empregados, e uma maior responsabilidade. Além disso, requer procedimentos eficazes para que a administração monitore os resultados e possa, desse modo, aceitar ou rejeitar decisões, quando necessário. Com as melhores decisões orientadas ao mercado, a delegação pode aumentar a quantidade de decisões indesejáveis ou não antecipadas. Por exemplo, se um gerente de vendas regional decide que a autorização para vender com um desconto de 35% no preço de tabela justifica um desconto temporário de 4% para ganhar participação de mercado, a administração deverá saber dessas decisões com antecedência para poder aceitá-las ou rejeitá-las.

O ambiente interno é bem influenciado até o ponto que as pessoas reconhecem que serão responsabilizadas. Este conceito é perfeitamente verdadeiro para o Presidente, o qual, com a supervisão do conselho de administração, tem a responsabilidade final de todas as atividades em uma organização.

Os princípios adicionais relacionados a funções e responsabilidades das partes que integram o gerenciamento de riscos corporativos eficaz são descritos no capítulo “Funções e Responsabilidades”.

Padrões de Recursos Humanos

Os processos relacionados a recursos humanos, como admissão, orientação, treinamento, avaliação, aconselhamento, promoção, compensação e adoção de medidas corretivas, enviam mensagens aos empregados; em relação aos níveis esperados de integridade, comportamento ético e competência. Por exemplo, normas de admissão dos indivíduos mais qualificados, com ênfase no histórico educacional, experiência de trabalho anterior, realizações anteriores, bem como comprovação da integridade e do comportamento ético, demonstrarão o compromisso de uma entidade com o profissional competente e digno de confiança. Isso é verdadeiro se as práticas de recrutamento incluem entrevistas formais de profundidade e treinamento na história da organização, sua cultura e seu estilo operacional.

Políticas de treinamento podem reforçar os níveis de desempenho esperados e o comportamento ao comunicarem as funções e as responsabilidades em perspectiva, bem como ao incluir práticas como cursos de treinamento e seminários, simulações de estudos de caso e exercícios de desempenho de papéis. Transferências e promoções fundamentadas em avaliações de desempenho demonstram o empenho da organização com o progresso dos empregados qualificados. Programas de compensação competitiva que incluem incentivos sob a forma de bonificações servem para motivar e reforçar os desempenhos de nível elevado – a despeito do fato de que os sistemas de prêmios devam ser estruturados e ter seus controles implementados para evitar tentações indevidas de efetuar manipulações de resultados. As medidas disciplinares transmitem a mensagem que as infrações aos comportamentos esperados não serão toleradas.

É essencial que os empregados estejam preparados para enfrentar novos desafios na medida em que as questões e os riscos por meio da organização modificam-se e adquirem maior complexidade - em parte devido à rápida mudança de tecnologias e da intensificação da concorrência. Ensino e treinamento, sejam eles mediante instruções na sala de aula, no auto-estudo ou treinamento na própria função devem contribuir para que o pessoal mantenha-se atualizado e trate com eficácia um ambiente em fase de transição. Não é suficiente admitir pessoal competente e fornecer-lhe treinamento somente uma vez. O processo de aprendizado é contínuo.

Implicações

Nunca é demais ressaltar a importância do ambiente interno de uma organização e o impacto positivo ou negativo que poderá causar sobre os componentes do gerenciamento de riscos corporativos. O impacto de um ambiente interno ineficaz pode ir muito longe e talvez provocar prejuízos financeiros, desgastes da imagem pública ou, até mesmo, o fracasso.

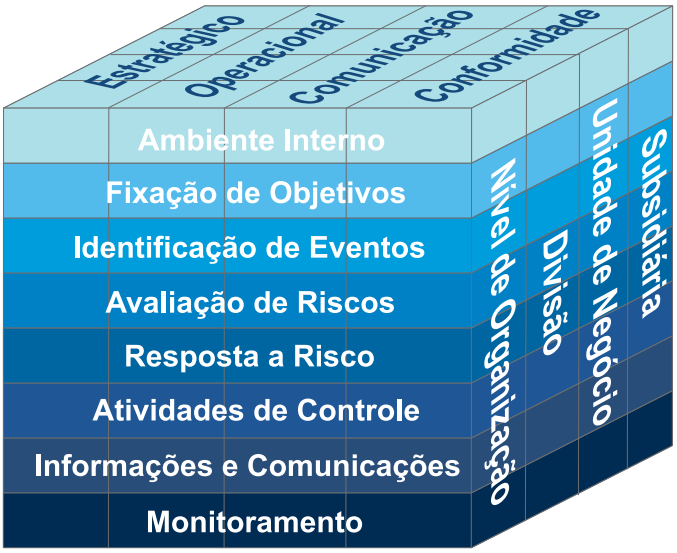
Lembrando o caso de uma corporação de energia que acreditava ser detentora de um gerenciamento de riscos corporativos eficaz, visto que possuía executivos qualificados e respeitados, um conselho de administração de prestígio, estratégia inovadora, sistemas de informações e atividades de controle adequadas, extensos manuais de políticas sobre as funções de riscos e de controle, bem como rotinas detalhadas de reconciliação e supervisão. Contudo, o seu ambiente interno apresentava graves defeitos. A administração participava de negócios duvidosos e o conselho de administração fazia vista grossa. Quando se descobriu que a Companhia havia distorcido resultados financeiros, a mesma perdeu a confiança dos acionistas, sofreu uma crise de liquidez e de destruição de seus ativos. Finalmente, a Companhia sofreu uma das maiores falências da história.

Para que uma organização possa desfrutar de um gerenciamento de riscos corporativos eficaz, a atitude e o interesse da alta administração devem ser claros e definitivos, bem como permear toda a organização. Não é suficiente apenas dizer as palavras corretas, uma atitude de “faça o que digo e não o que faço”, somente gerará um ambiente inadequado.


MCMXLV
SANTOS DUMONT
SANTOS DUMONT

3. Fixação de Objetivos

Resumo do Capítulo: Os objetivos são fixados no âmbito estratégico, estabelecendo uma base para os objetivos operacionais, de comunicação e os cumprimento de normas. Toda organização enfrenta uma variedade de riscos oriundos de fontes externas e internas, sendo a fixação de objetivos um pré-requisito à identificação eficaz de eventos, a avaliação de riscos e resposta a risco. Os objetivos são alinhados com o apetite a risco, o qual direciona os níveis de tolerância a riscos para a organização.



A fixação de objetivos é uma precondição à identificação de evento, à avaliação de riscos e às respostas aos riscos. Em primeiro lugar, é necessário que os objetivos existam para que a administração possa identificar e avaliar os riscos quanto a sua realização, bem como adotar as medidas necessárias para administrá-los.

Objetivos Estratégicos

A missão de uma organização estabelece, em sentido mais amplo, aquilo que a organização deseja alcançar. Não importa o termo utilizado, como “missão”, “visão”, ou “propósito”, é importante que a alta administração, sob a supervisão do conselho de administração, estabeleça explicitamente os motivos da existência da organização em um sentido amplo. A partir desses motivos, a alta administração fixa objetivos estratégicos, formula estratégias e estabelece os objetivos da organização relativos às operações, à conformidade e à comunicação. Embora a missão e os objetivos estratégicos de uma organização, geralmente, sejam estáveis, a sua estratégia e muitos de seus objetivos operacionais são mais dinâmicos e ajustam-se às condições internas e externas presentes. Na medida em que essas condições modificam-se, as estratégias e os objetivos operacionais são re-alinhados aos objetivos estratégicos.

Os objetivos estratégicos são metas de nível geral, alinhadas com a missão/visão da organização e fornecendo-lhe apoio. Os objetivos estratégicos refletem em como a alta administração escolheu uma forma de gerar valor para as partes interessadas.

Ao considerar as várias alternativas de alcançar os seus objetivos estratégicos, a alta administração identifica os riscos associados com uma ampla gama de escolhas estratégicas e analisa as suas implicações. Várias técnicas de identificação de eventos e de avaliação de riscos, discutidas a seguir e, podem ser utilizadas no processo de fixação de estratégias e objetivos.

Objetivos Correlatos

Estabelecer os objetivos corretos, que dão suporte e estejam alinhados com a estratégia selecionada, e associados a todas as atividades da organização é fator crítico de êxito. Ao orientar o seu enfoque, primeiramente, para os objetivos estratégicos e para a tática, a organização estará pronta para definir os objetivos correlatos no âmbito da organização, cuja realização gerará e preservará valor. Os objetivos no âmbito da organização são associados e integrados a objetivos mais específicos que fluem em cascata por meio da organização para os subobjetivos estabelecidos para várias atividades, como vendas, produção e funções de engenharia e infra-estrutura.

Ao fixar objetivos nos âmbitos da organização e de atividade, pode-se identificar fatores críticos para seu êxito. Os fatores críticos são fundamentais para que as metas sejam alcançadas. Os fatores críticos para o êxito existem em uma entidade, unidade de negócios, função, departamento ou pessoa física. Ao fixar objetivos, a administração poderá identificar critérios de mensuração do desempenho com um enfoque voltado para os fatores críticos de êxito.

Se os objetivos mostram-se consistentes com as práticas e o desempenho anteriores, a associação entre as atividades é conhecida. Entretanto, se os objetivos afastam-se das práticas anteriores da organização, cabe à direção identificar os vínculos ou enfrentar maiores riscos. Nesses casos, haverá uma necessidade ainda maior de haver objetivos e subobjetivos para a unidade de negócios coerentes com a nova orientação.

Os objetivos precisam ser mensuráveis e entendidos prontamente. O gerenciamento de riscos corporativos requer que o pessoal em todos os níveis tenha um entendimento indispensável em relação aos objetivos da organização na medida em que estes relacionem-se com a esfera de influência do indivíduo. Todos os empregados necessitam entender o que deverá ser realizado e, ainda, dispor de meios de mensuração daquilo que está sendo realizado.

Categorias de Objetivos Correlatos

Apesar da diversidade dos objetivos nas organizações, podemos estabelecer certas categorias mais amplas:

- Objetivos Operacionais – relacionam-se com a eficácia e a eficiência das operações da organização, inclusive metas de desempenho e de lucro, bem como reservas de recursos contra prejuízos. Variam de acordo com a decisão da administração em relação à estrutura e ao desempenho.
- Objetivos de Comunicação – relacionam-se com a confiabilidade dos relatórios. Incluem relatórios internos e externos e podem, ainda, conter informações financeiras e não financeiras.
- Objetivos de Conformidade – relacionam-se com o cumprimento de leis e regulamentos. Em alguns casos dependem de fatores externos e tendem a ser semelhantes em todas as organizações, e em outros casos em todo um setor industrial.

Determinados objetivos acompanham o ramo de negócios em que a organização se encontra. Algumas companhias, por exemplo, apresentam informações a órgãos ambientais, e Companhias com ações negociadas em bolsas de valores enviam informações para as autoridades normativas de valores mobiliários. Esses requisitos impostos externamente são estipulados por lei ou regulamentação e classificam-se nas categorias de Comunicação ou Conformidade, ou, ainda, como nos exemplos acima, em ambos.

Por outro lado, os objetivos operacionais e os destinados aos relatórios gerenciais internos baseiam-se mais em preferências, opiniões e estilos de gestão. Podem apresentar variações significativas de organização para organização, pelo simples fato de que pessoas competentes e honestas podem selecionar diferentes objetivos.

Por exemplo, no que se refere a desenvolvimento de produto, uma organização decide ser inovadora, outra seguidora imediata, e outra retardatária morosa. Essas opções afetam a estrutura, as habilidades, a dotação de pessoal e os controles da função de pesquisa e desenvolvimento. Conseqüentemente, não existe um processo de formulação de objetivos ideal para todas as organizações.

Objetivos Operacionais

Os objetivos operacionais referem-se à eficácia e à eficiência das operações da organização. Compreendem os subobjetivos correlatos de operações, com a finalidade de aprimorar a eficácia e a eficiência operacional que impulsionarão a organização na direção de sua meta final.

É necessário que os objetivos operacionais reflitam as condições específicas do negócio, da indústria e da economia, nas quais a organização atua. Os objetivos necessitam, por exemplo, ser pertinentes às pressões da concorrência em termos de qualidade, redução do ciclo para trazer os produtos ao mercado, ou mudanças em tecnologia. A administração deve assegurar-se que os objetivos reflitam a realidade e as exigências do mercado, bem como sejam expressos para que possibilitem uma medição prática de desempenho. Um conjunto nitidamente definido de objetivos operacionais, associados aos subobjetivos, é fundamental para o êxito da organização. Os objetivos operacionais possibilitam um ponto de referência para o direcionamento dos recursos alocados; se os objetivos operacionais de uma organização não forem claros ou adequadamente formulados, os seus recursos poderão ser mal aproveitados.

Objetivos de Comunicação

Uma comunicação confiável provê à administração informações exatas e completas, adequadas ao que se propõe. A comunicação oferece suporte ao processo decisório da administração e ao acompanhamento das atividades e do desempenho da organização. Alguns exemplos dos referidos relatórios incluem os resultados de programas de marketing, os relatórios diários sucintos de estimativas de resultados de vendas, a qualidade da produção e os resultados da satisfação dos empregados e dos clientes. A comunicação também relaciona-se com os relatórios preparados para divulgação externa, como demonstrações financeiras e divulgação em notas explicativas, discussão e análise da administração, e relatórios entregues a entidades normativas.

Objetivos de Conformidade

As organizações devem conduzir as suas atividades, bem como, adotar, freqüentemente, medidas específicas, de acordo com as leis e os regulamentos pertinentes. Esses requisitos podem relacionar-se a mercados, preço, impostos, meio-ambiente, bem-estar social de empregados e comércio internacional. As leis e os regulamentos aplicáveis estabelecem padrões mínimos de comportamento, que a organização integra em seus objetivos de conformidade. Por exemplo, as leis de saúde ocupacional e segurança podem levar uma organização a definir o seu objetivo como “Embalar e rotular todos os produtos químicos de acordo com as normas”. Nesse caso, as políticas e os procedimentos referem-se a programas de comunicação, inspeções locais e treinamento. O histórico de conformidade de uma organização poderá afetar de modo significativo, positivo ou negativo, a sua reputação na comunidade e no mercado.

Subcategorias

As categorias de objetivos fazem parte da linguagem comum estabelecida por essa estrutura, facilitando, dessa maneira, o entendimento e a comunicação. Porém, a organização poderá julgar conveniente discutir um subconjunto de uma ou mais categorias de objetivos para facilitar a comunicação interna ou externa, em relação a um tópico mais restrito. A organização poderá, por exemplo, decidir comunicar a eficácia de uma parte da categoria do relatório, por exemplo, gestão de riscos corporativos sobre comunicação externa, ou talvez apenas em relação à publicação de relatórios financeiros. Esse procedimento permite que a comunicação mantenha-se no contexto da estrutura de administração de riscos dessa organização, ao mesmo tempo em que permite comunicações de subconjuntos específicos de categorias.

Sobreposição de Objetivos

Um objetivo em uma categoria poderá sobrepor-se ou, ainda, auxiliar um objetivo em outra categoria. A categoria na qual um objetivo poderá cair depende às vezes das circunstâncias. Por exemplo, o fornecimento de informações confiáveis para que a administração de uma unidade de negócios administre e controle suas atividades de produção poderá servir para o cumprimento dos objetivos de operações e comunicação. E, na medida em que as informações são utilizadas para relatar dados ambientais ao governo, elas servirão de objetivos de conformidade.

Algumas organizações utilizam outra categoria de objetivos, “salvaguarda de recursos” às vezes chamado de “salvaguarda de bens,” o qual se sobrepõe em relação a outras categorias de objetivos. De um modo mais amplo, esses objetivos tratam de evitar a perda de bens ou recursos da organização, seja ela por meio de furto, desperdício, ineficiência ou simplesmente de decisões

comerciais falhas – como vender um produto a preço demasiado baixo, deixar de manter empregados de importância fundamental ou de evitar infrações a patentes, ou, ainda, incorrer em responsabilidades imprevistas. Esses objetivos são, essencialmente, de natureza operacional, embora determinados aspectos de salvaguarda possam cair em outras categorias. Nos casos da aplicação de exigências legais ou regulamentares, os referidos objetivos tornam-se itens de conformidade. Por outro lado, se o registro adequado reflete claramente nas perdas de bens nas demonstrações financeiras da organização, ele representará um objetivo de comunicação.

Quando considerados em conjunto com informes públicos, utiliza-se uma definição mais rigorosa para a salvaguarda de bens, que trata da prevenção ou da constatação oportuna de aquisição, do uso ou da alienação não autorizada dos bens de uma organização. Para discussões mais detalhadas dessa categoria de objetivos, consulte “Controle Interno – Estrutura Integrada”, inclusive o aditivo ao módulo de divulgações a “Partes Externas”.

Realização de Objetivos

Um processo adequado para a fixação de objetivos representa um componente crítico do gerenciamento de riscos corporativos. Embora os objetivos propiciem as metas mensuráveis na direção das quais a organização move-se ao realizar suas atividades, eles possuem diferentes graus de importância e prioridade. Da mesma forma, a despeito do fato de que uma organização deva dispor de uma garantia razoável de que determinados objetivos serão alcançados, nem sempre é esse o caso em relação a todos os objetivos.

O gerenciamento de riscos corporativos eficaz oferece garantia razoável de que os objetivos de comunicação estão sendo alcançados. Da mesma forma, deverá haver garantia razoável de que os objetivos de conformidade estão sendo alcançados. De um modo geral, o alcance dos objetivos de comunicação e conformidade está sob o controle da organização. Em outras palavras, uma vez determinados os objetivos, a organização terá total controle sobre a sua capacidade de fazer o que for necessário para atingi-los.

Porém, há uma diferença quando se trata de objetivos estratégicos e operacionais, em razão do cumprimento destes não estar sob controle exclusivo da organização. Uma organização poderá apresentar o desempenho previsto, mas, apesar disso, perder em desempenho para um concorrente. Ela está sujeita a eventos externos, como mudança de governo, condições climáticas adversas e assim por diante, em que as ocorrências fogem ao seu controle. Alguns desses eventos poderão ter sido considerados em seu processo de fixação de objetivos e tratados como se fossem pouco prováveis de ocorrer e com um plano de contingência caso ocorressem. Contudo, um plano como esse apenas consegue reduzir o impacto dos eventos externos e não garante que os objetivos serão alcançados.

O gerenciamento de riscos corporativos referentes a operações concentra-se basicamente em desenvolver consistência para os objetivos e as metas em toda a organização, identificar fatores e riscos fundamentais de êxito, avaliar os riscos e desenvolver respostas bem fundamentadas, implementar respostas adequadas a riscos e estabelecer controles e relatórios do desempenho e expectativas no momento oportuno. No caso dos objetivos estratégicos e operacionais, o gerenciamento de riscos corporativos poderá oferecer garantia razoável de que a diretoria executiva e o conselho de administração, em seu papel de supervisão, são informados oportunamente até que ponto a organização está se movimentando na direção do cumprimento desses objetivos.

Objetivos Selecionados

Como parte do gerenciamento de riscos corporativos, a administração não apenas seleciona objetivos e considera o modo pelo estes darão suporte à missão da organização, mas também certifica-se que esses objetivos estão em conformidade com o apetite a risco. Um alinhamento falho poderá fazer que os riscos aceitos sejam demasiadamente baixos para alcançar os objetivos, ou, por outro lado, que aceite riscos em demasia. O gerenciamento de riscos corporativos eficaz não dita os objetivos que a administração deve escolher, mas certifica-se que a referida administração dispõe de um processo que alinhe objetivos estratégicos com a sua missão e que esses objetivos e os correlatos selecionados estejam de acordo com o apetite a risco.

Apetite a risco

O apetite a risco estabelecido pela administração, mediante supervisão do conselho de administração, é um marco de referência na fixação de estratégias. As organizações podem definir o apetite a risco como um equilíbrio aceitável entre crescimento, riscos e retorno, ou como medidas de valor agregado de acionistas ajustadas aos riscos. Determinadas entidades, como as organizações sem fins lucrativos, definem apetite a risco como o nível de riscos que aceitarão ao oferecer valor para as suas partes interessadas.

Existe uma relação entre o apetite a risco de uma organização e a sua estratégia. Via de regra, entre as diferentes estratégias, qualquer uma poderá ser designada para alcançar as metas desejadas de crescimento e retorno, cada qual com seus respectivos riscos. O gerenciamento de riscos corporativos aplicado ao se estabelecer estratégias ajuda a administração a selecionar uma que seja compatível com o seu apetite a risco. Se os riscos associados a uma estratégia forem incompatíveis com o que a organização estabeleceu, esta terá de ser revisada. Isso poderá ocorrer nos casos em que a administração inicialmente formula uma estratégia que ultrapassa esse limite, ou em que a estratégia não inclua riscos suficientes que lhe permitam alcançar seus objetivos estratégicos e cumprir sua missão.

O apetite a risco de uma organização reflete-se na sua estratégia que, por sua vez, impulsiona a alocação de recursos. A administração aloca recursos nas unidades de negócios, considerando o apetite a risco e os planos estratégicos para cada uma das unidades de negócios, para gerar o retorno desejado dos recursos investidos. A administração tenta alinhar a organização, o pessoal, os processos e a infra-estrutura para facilitar o êxito da implementação e permitir que se mantenha dentro dos parâmetros de seu apetite a risco.

Tolerância a Risco

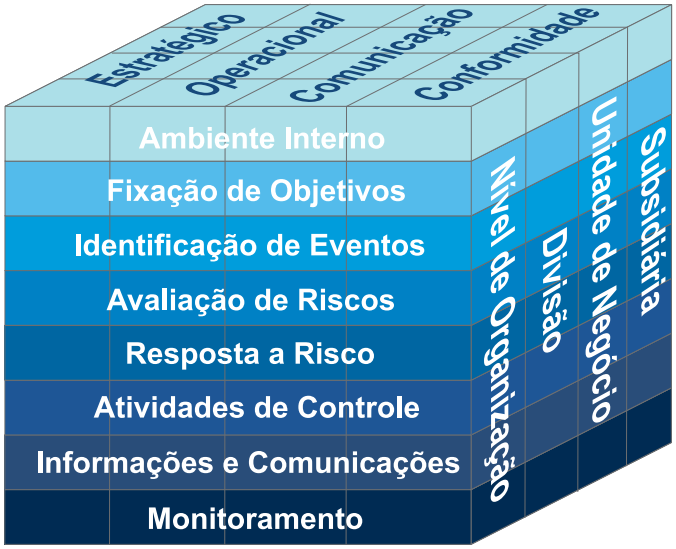
A tolerância a risco é o nível de variação aceitável quanto à realização de um determinado objetivo. As tolerâncias aos riscos podem ser mensuradas e, freqüentemente, com as mesmas unidades de medida aplicadas às metas dos objetivos associados.

As medidas de desempenho são empregadas para assegurar que os resultados efetivamente obtidos estarão dentro dos limites estabelecidos pela tolerância a risco. Por exemplo, uma companhia fixa a sua meta de entregas pontuais em 98%, com uma variação aceitável na faixa de 97% a 100% das vezes.Sua meta de treinamento prevê um índice de aprovação de 90%, com um desempenho aceitável de pelo menos 75%, e espera que o pessoal responda a todas as reclamações de clientes dentro de 24 horas, mas aceita que até 25% das reclamações poderão receber uma resposta entre 24 e 36 horas.

Ao definir a tolerância a risco, a administração considera a importância relativa dos objetivos associados e alinha o seu conjunto ao apetite a risco. Uma operação dentro dos parâmetros de tolerâncias a riscos possibilita à administração maior garantia de que a Companhia permanecerá dentro de seu apetite a risco, o qual, por sua vez, possibilita um grau mais elevado de confiança para que os seus objetivos possa ser atingidos.

4. Identificação de Eventos

Resumo do capítulo: a administração identifica os eventos em potencial que, se ocorrerem, afetarão a organização e determina se estes representam oportunidades ou se podem ter algum efeito adverso na sua capacidade de implementar adequadamente a estratégia e alcançar os objetivos. Eventos de impacto negativo representam riscos que exigem avaliação e resposta da administração. Os eventos de impacto positivo representam oportunidades que são canalizadas de volta aos processos de fixação das estratégias e dos objetivos. Ao identificar eventos, a administração considera uma variedade de fatores internos e externos que podem dar origem a riscos e a oportunidades no contexto de toda a organização.



Eventos

Eventos são incidentes ou ocorrências originadas a partir de fontes internas ou externas que afetam a implementação da estratégia ou a realização dos objetivos. Os eventos podem provocar impacto positivo, negativo ou ambos.

Ao identificar os eventos, a administração deve reconhecer que existem determinadas incertezas, mas não sabe se um evento ocorrerá, quando poderá ocorrer, nem o impacto que terá caso aconteça. Inicialmente, a administração considera uma faixa de eventos em potencial, originadas de fontes internas e externas, sem levar em conta se o impacto será favorável ou desfavorável. Desse modo, a administração poderá identificar não apenas eventos com potencial impacto negativo, mas também aqueles que representam oportunidades a serem aproveitadas.

Os eventos variam do óbvio ao obscuro, e vão de zero a altamente significativo. Para evitar que um evento deixe de ser percebido, recomenda-se identificá-lo de forma independente à da avaliação de sua probabilidade de ocorrência e de seu impacto, que fazem parte do tópico “Avaliação de Riscos”. Contudo, existem limitações de ordem prática, e geralmente é difícil saber por onde passa essa linha. Todavia, mesmo os eventos com possibilidade de ocorrência relativamente baixa não devem ser ignorados se o impacto na realização de um objetivo importante for elevado.

Fatores Influenciadores

Uma infinidade de fatores externos e internos impulsiona os eventos que afetam a implementação da estratégia e o cumprimento dos objetivos. Como parte do gerenciamento de riscos corporativos, a administração reconhece a importância de compreender esses fatores e o tipo de evento que pode emanar deles. Os fatores externos, com os exemplos de eventos correlatos e as suas implicações, incluem o seguinte:

Identificação de Eventos

- Econômicos – os eventos relacionados contemplam: oscilações de preços, disponibilidade de capital, ou redução nas barreiras à entrada da concorrência, cujo resultado se traduz em um custo de capital mais elevado ou mais reduzido, e em novos concorrentes.
- Meio ambiente – refere-se aos seguintes eventos: incêndios, inundações ou terremotos, que provocam danos a fábricas ou edificações, restrição quanto ao uso de matérias-primas e perda de capital humano.
- Políticos – eleição de agentes do governo com novas agendas políticas e novas leis e regulamentos, resultando, por exemplo, na abertura ou na restrição ao acesso a mercados estrangeiros, ou elevação ou redução na carga tributária.
- Sociais – são alterações nas condições demográficas, nos costumes sociais, nas estruturas da família, nas prioridades de trabalho/vida e a atividade terrorista, que, por sua vez, podem provocar mudanças na demanda de produtos e serviços, novos locais de compra, demandas relacionadas a recursos humanos e paralisações da produção.
- Tecnológicos – são novas formas de comércio eletrônico, que podem provocar aumento na disponibilidade de dados, reduções de custos de infra-estrutura e aumento da demanda de serviços com base em tecnologia.

Os eventos também originam-se das escolhas que a administração faz em relação ao seu funcionamento. A capacidade e habilidade de gestão da organização refletem suas escolhas passadas, influenciam eventos futuros e afetam as decisões gerenciais. Os fatores internos e os exemplos de eventos correlatos e de suas implicações incluem o seguinte:

- Infra-estrutura – aumento da alocação de capital em manutenção preventiva e suporte ao call center, reduzindo o tempo de paralisação de equipamentos e aumentando a satisfação do cliente.
- Pessoal – acidentes de trabalho, atividades fraudulentas e expiração de acordos de trabalho, causando redução de pessoal disponível, danos pessoais, monetários ou à reputação da organização e paralisações da produção.
- Processo – modificações de processos sem alteração adequada nos protocolos administrativos, erros de execução de processo e terceirização da entrega a clientes sem uma supervisão adequada, implicando perda de participação de mercado, ineficiência, insatisfação do cliente e diminuição da fidelidade deste.
- Tecnologia – aumento de recursos para fazer face à variabilidade de volume, violações da segurança e paralisação, em potencial, de sistemas, provocando redução da carteira de pedidos, transações fraudulentas e incapacidade de se manter as operações.

A identificação dos fatores externos e internos que o influenciam é útil para a constatação efetiva dos eventos. Uma vez identificados os principais fatores, a administração poderá considerar o seu significado e concentrar-se nos eventos capazes de afetar a realização dos objetivos.

Um fabricante e importador de calçados, por exemplo, estabeleceu a missão de tornar-se líder na indústria de calçados masculinos de alta qualidade. Para realizar esse objetivo, começou a fabricar produtos que aliavam estilo, conforto e durabilidade, usando técnicas mais avançadas e materiais de fornecedores estrangeiros rigorosamente selecionados. A Companhia analisou o ambiente operacional externo e identificou fatores sociais e seus respectivos eventos, como a mudança da faixa etária de seu principal mercado consumidor e as tendências para roupas de trabalho. Os eventos originados por fatores econômicos incluíam flutuações de moeda estrangeira e oscilações nas taxas de juros. Os fatores tecnológicos internos indicavam um sistema obsoleto de gestão de distribuição e, os fatores internos de pessoal, de treinamento inadequado em marketing.

Além de constatados no âmbito da organização, os eventos também devem ser identificados no nível da atividade. Esse procedimento contribui para orientar o enfoque do gerenciamento de riscos (o assunto do próximo capítulo) às principais unidades de negócios ou funções, como vendas, produção, marketing, tecnologia da informação e pesquisa e desenvolvimento.

Técnicas de Identificação de Eventos

A metodologia de identificação de eventos de uma organização poderá empregar uma combinação de técnicas com ferramentas de apoio. Por exemplo, a administração poderá tornar os seminários interativos em grupo como parte de seu método de identificação de eventos, com um facilitador que utilizará alguma ferramenta para assessorar os participantes.

As técnicas de identificação de eventos examinam tanto o passado quanto o futuro. As técnicas voltadas a eventos passados e tendências consideram questões como o histórico de falta de pagamento, as mudanças em preços de *commodities* e os acidentes que implicaram perda de tempo. As técnicas que enfocam eventos sobre exposições futuras consideram questões como mudanças nas características demográficas, novas condições de mercado e ações da concorrência.

Essas técnicas podem apresentar grande variação quanto à sofisticação; enquanto muitas das técnicas mais sofisticadas são específicas ao próprio ramo de atividades, a maior parte é obtida mediante uma abordagem simples. Por exemplo, tanto as indústrias de serviços financeiros, de saúde e de segurança empregam técnicas de rastreamento de eventos de perda. Essas técnicas iniciam-se com foco no histórico de eventos comuns – nos quais as abordagens mais simples analisam eventos com base em percepções internas dos empregados, pois as técnicas mais avançadas baseiam-se em fontes factuais de eventos observáveis – para, então, alimentar esses dados em modelos de projeção altamente sofisticados. As organizações mais avançadas em termos de gerenciamento de riscos corporativos utilizam uma combinação de técnicas que aliam eventos passados e potenciais eventos futuros.

As técnicas também variam de acordo com o nível onde são utilizadas na organização. Algumas delas utilizam a análise detalhada de dados e criam uma visão de eventos de baixo para cima, enquanto outras, a visão de cima para baixo. O Anexo 4.1 apresenta exemplos de técnicas de identificação de eventos.

Anexo 4.1

- Inventário de eventos – trata-se da relação detalhada de eventos em potencial comuns às organizações de um cenário industrial, ou para um determinado tipo de processo, ou atividade, comum às indústrias. Alguns softwares podem gerar listas de eventos relevantes originárias de uma base geral de potenciais eventos, que servirão como ponto de partida para se identificar eventos. Por exemplo, uma organização envolvida em um projeto de desenvolvimento de software utiliza-se de uma relação detalhada de possíveis eventos referentes a projetos desse tipo.
- Análise interna – pode ser realizada como parte da rotina do ciclo de planejamento de negócios, tipicamente por meio de reuniões dos responsáveis pela unidade de negócios. A análise interna pode dispor das informações de outras partes interessadas (clientes, fornecedores e outras unidades de negócios) ou da consulta a um especialista no assunto, e de fora da unidade (especialistas funcionais internos ou externos ou pessoal interno de auditoria). Por exemplo, ao considerar o lançamento de um novo produto, uma organização usa sua própria experiência histórica em conjunto com a pesquisa de mercado para identificar eventos que tenham afetado o grau de êxito dos produtos da concorrência.

- Alçadas e limites – esses gatilhos servem para alertar a administração sobre áreas de preocupação pela comparação de transações ou ocorrências atuais com critérios predefinidos. Uma vez acionado o gatilho, um evento poderá necessitar de nova avaliação ou de uma resposta imediata. Por exemplo, a administração de uma organização monitora o volume de vendas nos mercados determinados para receber novos programas de marketing ou publicitários e redireciona seus recursos com base nos resultados. Outra organização pesquisa as estruturas de preços da concorrência e considera a hipótese de alterar os seus próprios preços se um limite específico for atingido.

- Seminários e entrevistas com facilitadores – essas técnicas identificam eventos com base na experiência e no conhecimento acumulado da administração, do pessoal ou de outras partes interessadas por meio de discussões estruturadas. O facilitador liderará um debate sobre eventos que possam afetar a realização dos objetivos de uma organização ou unidade. Por exemplo, um controller financeiro conduz um seminário com os membros da equipe de contabilidade para identificar eventos capazes de impactar os objetivos de comunicação externa das informações financeiras da organização. Ao combinar o conhecimento e a experiência dos membros da equipe, podem-se identificar importantes eventos que, de outro modo, poderiam passar despercebidos.

- Análise de fluxo de processo – essa técnica reúne as entradas, as tarefas, as responsabilidades e as saídas que se combinam para formar um processo. Considerando-se os fatores internos e externos que afetam as entradas ou as atividades em um processo, a organização identifica os eventos que podem afetar o cumprimento dos objetivos deste. Por exemplo, um laboratório médico mapeia os seus processos de recebimento e a análise de amostras de sangue. Ao utilizar mapas de processo, o laboratório considera uma série de fatores que podem afetar as entradas, as tarefas e as responsabilidades, identificando os riscos relacionados com a rotulagem de amostras, as transferências do fluxo dentro do processo e as mudanças de turno do pessoal.

- Indicadores preventivos de eventos – ao monitorar dados associados aos eventos, as organizações identificam a existência de condições que poderiam originar um evento. Por exemplo, as instituições financeiras, desde há muito, reconhecem a correlação entre os atrasos nos pagamentos de empréstimos e a eventual inadimplência nestes e o efeito positivo de uma intervenção precoce. O monitoramento de padrões de pagamento permite que o potencial de inadimplência seja reduzido por uma ação oportuna.

- Metodologias de dados sobre eventos de perda – as bases de dados sobre eventos individuais de perdas passados representam uma fonte útil de informações para identificar as tendências e a raiz dos problemas. Após ter identificado uma raiz, a administração poderá decidir que é mais eficaz avaliá-la e tratá-la do que abordar eventos individuais. Por exemplo, uma Companhia que opera uma grande frota de automóveis mantém uma base de dados de reclamações de acidentes e, mediante análise, constata que uma porcentagem desproporcional de acidentes, em número e valor monetário, está associada a motoristas de determinadas unidades, área geográfica e faixas etárias. Essa análise permite que a direção identifique as causas dos eventos e adote as medidas necessárias.

O grau de profundidade, de amplitude e de disciplina na identificação de eventos pode variar de uma organização para outra. A administração seleciona as técnicas compatíveis com a sua filosofia de gestão de riscos e assegura que a entidade desenvolve as funcionalidades necessárias de identificação de eventos e que as ferramentas de apoio estão implementadas. De um modo geral, a identificação necessita ser suficientemente eficaz pelo fato de ser a base dos componentes da avaliação de riscos e da resposta a estes.

Interdependências

Via de regra; os eventos não ocorrem de forma isolada. Um evento poderá desencadear outro, e ocorrer concomitantemente. Para identificar os eventos, a administração deve entender o modo pelo qual eles se inter-relacionam. A avaliação dos relacionamentos permite determinar em que pontos os esforços da gestão de riscos estarão bem direcionados. Por exemplo, uma mudança na taxa de juros do Banco Central afeta as taxas de câmbio, que é relevante aos ganhos e às perdas nas transações de moeda de uma organização. A decisão de reduzir o investimento em capital postergará um aperfeiçoamento dos sistemas de gestão de distribuição e ocasionará um tempo de paralisação adicional e uma elevação nos custos operacionais. A decisão de ampliar o treinamento em marketing poderá melhorar a força de vendas e a qualidade do serviço, trazendo como resultado um aumento na freqüência e no volume de pedidos de clientes. A decisão de entrar em uma nova linha de negócios, com grandes incentivos associados ao desempenho informado, poderá aumentar os riscos de erro na aplicação de princípios contábeis e demonstrações financeiras incorretas.

Categorias de Eventos

Pode ser útil agrupar os eventos em potencial em categorias. Ao agregar os eventos horizontalmente em uma organização e verticalmente nas unidades operacionais, a administração desenvolverá a compreensão do relacionamento entre os eventos e poderá adquirir melhores informações para formar uma base para avaliar riscos. Ao agrupar eventos semelhantes, a administração terá melhores condições de identificar oportunidades e riscos.

A classificação de eventos também permite à administração considerar o grau de completude de seus esforços de identificação de eventos. Por exemplo, uma organização poderá classificar os eventos relativos à cobrança de credores em uma única categoria, denominada Inadimplência – Credores. Ao examinar os eventos nessa categoria, a administração poderá verificar se realmente identificou todos os eventos em potencial e significativos relacionados com Inadimplência – Credores.

Algumas organizações estabelecem categorias de eventos com base na própria classificação de objetivos, utilizando uma hierarquia que se inicia nos objetivos em nível geral, para, então, fluir em cascata até os objetivos correlatos às unidades ou às funções organizacionais e aos processos.

O Anexo 4.2 ilustra uma abordagem utilizada para estabelecer as categorias de eventos dentro do contexto de fatores mais amplos internos e externos.

Anexo 4.2

Categorias de Eventos

Fatores Externos

Econômicos

- Disponibilidade de capital
- Emissões de crédito, inadimplência
- Concentração
- Liquidez
- Mercados financeiros
- Desemprego
- Concorrência
- Fusões / aquisições

Meio Ambiente

- Emissões e dejetos
- Energia
- Desastres naturais
- Desenvolvimento sustentável

Políticos

- Mudanças de governo
- Legislação
- Política pública
- Regulamentos

Sociais

- Características demográficas
- Comportamento do consumidor
- Cidadania corporativa
- Privacidade
- Terrorismo

Tecnológicos

- Interrupções
- Comércio eletrônico
- Dados externos
- Tecnologias emergentes

Fatores Internos

Infra-estrutura

- Disponibilidade de bens
- Capacidade dos bens
- Acesso ao capital
- Complexidade

Pessoal

- Capacidade dos empregados
- Atividade fraudulenta
- Saúde e segurança

Processo

- Capacidade
- Design
- Execução
- Dependências / fornecedores

Tecnologia

- Integridade de dados
- Disponibilidade de dados e sistemas
- Seleção de sistemas
- Desenvolvimento
- Alocação
- Manutenção

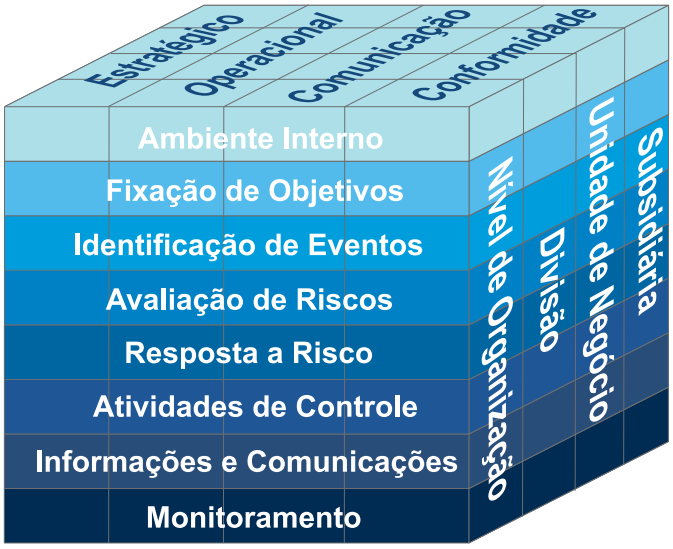
Diferenciação de Riscos e Oportunidades

Se um evento ocorre, ele terá um impacto negativo, ou positivo, ou, até mesmo, ambos. Os eventos cujo impacto é negativo representam riscos que exigem avaliação e resposta da administração. Da mesma forma, o risco é a possibilidade de que um evento ocorra e prejudique a realização dos objetivos.

Os eventos cujo impacto é positivo representam oportunidades ou contrabalançam os impactos negativos dos riscos. Oportunidade é a possibilidade de que um evento ocorra e influencie favoravelmente na realização dos objetivos, apoiando, desse modo, a criação de valor. Os eventos que representam as oportunidades são canalizados de volta para os processos de fixação de estratégias ou de objetivos por parte da administração, para que se formulem ações para o aproveitamento dessas oportunidades. Os eventos que neutralizam o impacto negativo dos riscos são levados em conta na avaliação de riscos e da resposta a estes.

5. Avaliação de Riscos

Resumo do capítulo: a avaliação de riscos permite que uma organização considere até que ponto eventos em potencial podem impactar a realização dos objetivos. A administração avalia os eventos com base em duas perspectivas – probabilidade e impacto – e, geralmente, utiliza uma combinação de métodos qualitativos e quantitativos. Os impactos positivos e negativos dos eventos em potencial devem ser analisados isoladamente ou por categoria em toda a organização. Os riscos são avaliados com base em suas características inerentes e residuais.



Contexto para a Avaliação de Riscos

Fatores externos e internos influenciam os eventos que poderão ocorrer, e até que ponto os referidos eventos podem afetar os objetivos de uma organização. Embora alguns fatores sejam comuns às organizações, via de regra, os eventos resultantes são singulares em relação a uma determinada organização tendo em vista seus objetivos estabelecidos e decisões anteriores. Ao avaliar riscos, a administração considera o composto dos futuros eventos em potencial pertinentes à organização e às suas atividades no contexto das questões que dão forma ao perfil de riscos, como tamanho da organização, complexidade das operações e grau de regulamentação de suas atividades.

Ao avaliar riscos, a administração leva em consideração eventos previstos e imprevistos. Muitos eventos são rotineiros e recorrentes e já foram abordados nos programas de gestão e orçamentos operacionais, enquanto que outros são imprevistos. A administração avalia os riscos em potencial de eventos imprevistos e, caso ainda não tenha feito essa avaliação, até os previstos que podem causar um impacto significativo na organização.

Embora o termo “avaliação de riscos” tenha sido usado em conexão com uma atividade realizada, uma única vez, no contexto de “avaliação de riscos corporativos”, o componente de “avaliação de riscos” é uma interação contínua e repetida das ações que ocorrem em toda a organização.

Risco Inerente e Residual

A administração leva em conta tanto o risco inerente quanto o residual. Risco inerente é o risco que uma organização terá de enfrentar na falta de medidas que a administração possa adotar para alterar a probabilidade ou o impacto dos eventos. Risco residual é aquele que ainda permanece após a resposta da administração. A avaliação de riscos é aplicada primeiramente aos riscos inerentes. Após o desenvolvimento das respostas aos riscos, a administração passará a considerar os riscos residuais.

Estimativa da Probabilidade e do Impacto

A incerteza de eventos em potencial é avaliada a partir de duas perspectivas – probabilidade e impacto. A probabilidade representa a possibilidade de que um determinado evento ocorrerá, enquanto o impacto representa o seu efeito. Probabilidade e impacto são termos de uso comum, embora algumas organizações utilizem termos, como probabilidade, severidade, gravidade ou conseqüência. Às vezes os termos assumem conotações mais específicas, como é o caso de *likelihood*[2], usado para indicar a possibilidade de que um evento ocorra em termos qualitativos, como elevada, média e reduzida ou outros critérios de escalas, e de *probability*, indica uma medida quantitativa, como porcentagem, freqüência de ocorrência ou outra medida numérica.

A determinação do grau de atenção depende da avaliação de uma série de riscos que uma organização enfrenta, e isso é uma tarefa difícil e desafiadora. A administração reconhece que um risco com reduzida probabilidade de ocorrência e baixo potencial de impacto, geralmente, não requer maiores considerações. Por outro lado, um risco com elevada probabilidade de ocorrência e um potencial de impacto significativo demanda atenção considerável. As circunstâncias situadas entre esses extremos geralmente são difíceis de julgar. É importante que a análise seja racional e cuidadosa.

[2] N.T. Os termos “*likelihood*” e “*probability*” referem-se a um mesmo vocábulo em português, isto é, “probabilidade”. Consultar o glossário no final desta obra.

O horizonte de tempo empregado para avaliar riscos deverá ser consistente com o tempo das estratégias e objetivos relacionados a esses riscos. Em razão das estratégias e objetivos de muitas organizações considerarem horizontes de tempo de curta a média duração, a administração naturalmente concentra-se nos riscos associados com esses períodos de tempo. Contudo, alguns aspectos do direcionamento estratégico e dos objetivos estendem-se a prazo mais longo. Conseqüentemente, a administração precisa levar em conta os cenários de prazos mais longos para não ignorar riscos que possam estar mais adiante.

Por exemplo, uma Companhia que atua na Califórnia poderá considerar o risco de que um terremoto possa paralisar as suas operações comerciais. Sem um horizonte de tempo especificado para a avaliação de riscos, será elevada a probabilidade de um terremoto cuja intensidade na escala Richter seja superior a 6.0, talvez essa probabilidade esteja praticamente certa. Por outro lado, a probabilidade de que esse tipo de terremoto ocorra dentro de dois anos é, substancialmente, mais baixa. Ao estabelecer um horizonte de tempo, a organização adquire mais informação em relação à importância relativa do risco e uma maior habilidade para comparar diversos riscos.

Freqüentemente, a administração emprega medições de desempenho na determinação de quais objetivos estão sendo alcançados e, geralmente, utiliza uma mesma unidade de medida, ou uma unidade compatível ao considerar o impacto em potencial de um risco para a realização de um objetivo específico. Por exemplo, uma Companhia com um objetivo de manter um nível específico de serviço ao cliente terá arquitetado uma classificação ou outra medida para esse objetivo, como o índice de satisfação de cliente, quantidade de reclamações, ou quantidade de repetição de compras. Ao avaliar o impacto de um risco que poderia afetar o serviço ao cliente – como seria o caso da possibilidade de que o site da companhia pode manter-se indisponível por um certo tempo, o impacto será determinado melhor utilizando-se as mesmas medidas.

Fontes de Dados

Via de regra, as estimativas de probabilidade e grau de impacto de riscos são conduzidas utilizando dados de eventos passados observáveis, os quais fornecem uma base mais objetiva do que as estimativas inteiramente subjetivas. Os dados gerados internamente e embasados na experiência passada da própria organização, podem refletir qualidades pessoais menos subjetivas e propiciar melhores resultados do que os dados de fontes externas. Contudo, mesmo que os dados gerados internamente sejam um dado primário, os externos podem ser úteis como um ponto de controle, ou para aprimorar a análise. Por exemplo, a administração de uma organização, ao avaliar o risco de paralisações da produção em razão de falhas de equipamentos, verifica primeiramente a freqüência e o impacto de falhas anteriores de seus próprios equipamentos de manufatura. Em seguida, suplementa esses dados com indicadores de desempenho para a indústria. Esse procedimento possibilita uma estimativa mais precisa da probabilidade e do impacto de falhas, bem como, mais eficaz da manutenção preventiva. Deve-se ter cautela ao se utilizar eventos passados para fazer previsões futuras, visto que os fatores que influenciam os eventos podem modificar-se com o passar do tempo.

Perspectiva

Os gestores sempre fazem julgamentos subjetivos sobre a incerteza e ao julgar devem reconhecer as limitações inerentes. As constatações feitas na pesquisa psicológica indicam que os tomadores de decisão em diversas funções, inclusive administradores de corporações, mostram-se muito confiantes ao realizar estimativas e não reconhecem a quantidade de incerteza que realmente existe. Estudos demonstram um notável "viés de confiança excessiva," que leva a intervalos indevidamente estreitos para o impacto e as probabilidades estimadas, por exemplo, as metodologias de valor em risco. Essa tendência ao excesso de confiança ao estimar a incerteza pode ser minimizada pela utilização eficaz de dados empíricos obtidos externa ou internamente. Na falta desses dados, uma consciência aguçada da penetrabilidade do viés poderá ajudar a mitigar esses efeitos.

As tendências humanas relacionadas ao ato de decidir são apresentadas de outra forma, na qual não é incomum que as pessoas façam escolhas diferentes ao buscar ganhos a fim de evitar perdas. Ao reconhecer essas tendências humanas, o gestor pode destacar as informações para reforçar o apetite e o comportamento perante risco em toda a organização. A forma pela qual as informações são apresentadas ou "estruturadas" podem afetar significativamente a sua interpretação e a forma pela qual os riscos associados ou as oportunidades são vistos, conforme descrito no Anexo 5.1.

Anexo 5.1

As pessoas apresentam diferentes respostas a prejuízos em potencial comparando-os a ganhos em potencial. A forma pela qual um risco é estruturado – com o enfoque na parte de cima (um ganho em potencial) ou na parte de baixo (um prejuízo em potencial) – geralmente, influencia a resposta. A teoria de expectativas, a qual explora o processo decisório do ser humano, diz que as pessoas não se mostram neutras em relação aos riscos; ou melhor, uma resposta a prejuízo tende a ser mais extrema do que uma resposta a ganho. E com isso, vem a tendência de interpretar erradamente probabilidades e reações a soluções acertadas. Para ilustrar o raciocínio, uma pessoa deparar-se com dois conjuntos de opções:

1. Um ganho certo de $240 ou 25% de chance de ganhar $1.000, e 75% de chance de não ganhar nada.
2. Um prejuízo certo de $750, ou 75% de chance de perder $1.000, e 25% de chance de não perder nada

No primeiro conjunto de opções, a maioria escolheria "um ganho certo de $240," por causa de suas tendências de aversão a riscos em relação a ganhos e questões estruturadas positivamente. Por outro lado, a maioria escolheria "uma chance de 75% de perder $1.000," em razão de suas tendências de procurar riscos em relação a prejuízos e questões estruturadas negativamente. Segundo a teoria de expectativas, as pessoas não desejam colocar em risco o que já tem ou pensam que podem ter, porém apresentarão maior tolerância a riscos quando podem minimizar os prejuízos.

Técnicas de Avaliação

A metodologia de avaliação de riscos de uma organização inclui uma combinação de técnicas qualitativas e quantitativas. Geralmente, a administração emprega técnicas qualitativas de avaliação se os riscos não se prestam a quantificação, ou se não há dados confiáveis em quantidade suficiente para a realização das avaliações quantitativas, ou, ainda, se a relação custo-benefício para obtenção e análise de dados não for viável. Tipicamente, as técnicas quantitativas emprestam maior precisão e são utilizadas em atividades mais complexas e sofisticadas para suplementar as técnicas qualitativas.

As técnicas quantitativas de avaliação geralmente requerem mais esforço e rigor, muitas vezes utilizando modelos matemáticos não triviais. As técnicas quantitativas dependem sobremaneira da qualidade dos dados e das premissas adotadas e são mais relevantes para exposições que apresentem um histórico conhecido, uma freqüência de sua variabilidade e permitam uma previsão confiável. O Anexo 5.2 exemplifica as técnicas quantitativas de avaliação de riscos.

Anexo 5.2

- Comparação com Referências de Mercado (*Benchmarking*) – É um processo cooperativo entre um grupo de organizações. O benchmarking enfoca eventos ou processos específicos, compara medições e resultados utilizando métricas comuns, bem como identifica oportunidades de melhoria. Dados de eventos, processos e medidas são desenvolvidos para a comparação de desempenho. Algumas Companhias utilizam o *benchmarking* para avaliar a probabilidade e o impacto de eventos em potencial em uma indústria.
- Modelos Probabilísticos – Os modelos probabilísticos associam a uma gama de eventos e seu respectivo impacto, a probabilidade de ocorrência sob determinadas premissas. A probabilidade e o impacto são avaliados com base em dados históricos ou resultados simulados que refletem hipóteses de comportamento futuro. Os exemplos de modelos probabilísticos incluem valor em risco (*value-at-risk*), fluxo de caixa em risco, receitas em risco e distribuições de prejuízo operacional e de crédito. Os modelos probabilísticos podem ser utilizados com diferentes horizontes de tempo para estimar os seus resultados, como a faixa de prazos dos instrumentos financeiros disponíveis. Os modelos probabilísticos também podem ser usados para avaliar resultados esperados ou médias em relação a impactos imprevistos ou extremos.
- Modelos Não Probabilísticos – Os modelos não probabilísticos empregam critérios subjetivos para estimar o impacto de eventos, sem quantificar uma probabilidade associada. A avaliação do impacto de eventos baseia-se em dados históricos ou simulados a partir de hipóteses sobre o comportamento futuro. Os exemplos de modelos não probabilísticos incluem medições de sensibilidade, testes de estresse e análises de cenários.

Para obter consenso sobre a probabilidade e o impacto de eventos de risco pelo uso de técnicas qualitativas de avaliação, as organizações poderão utilizar a mesma abordagem que usam na identificação dos eventos, como entrevistas e seminários. Um processo de auto-avaliação de riscos colhe as opiniões dos participantes a respeito da probabilidade em potencial e do impacto de eventos futuros, utilizando escalas descritivas ou numéricas.

Uma organização não necessita empregar as mesmas técnicas de avaliação para todas as suas unidades de negócios. Em vez disso, a escolha das técnicas deverá refletir na necessidade de exatidão e na cultura da unidade de negócios. Em uma Companhia, por exemplo, ao identificar e avaliar riscos no âmbito de processo, uma unidade de negócios emprega questionários de auto-avaliação, enquanto outra usa seminários. Os riscos são avaliados com base na característica inerente ou residual dos riscos, para então serem organizados e agrupados por categorias de risco e objetivos para ambas as unidades de negócios. Embora diferentes métodos sejam empregados, eles permitem consistência suficiente para facilitar a avaliação de riscos em toda a organização.

A administração pode obter uma medida quantitativa do impacto de um evento para toda a organização, quando todas as avaliações individuais de riscos com relação ao mesmo evento estiverem expressas em termos quantitativos. Por exemplo, o impacto de uma alteração nos preços de energia sobre a margem bruta é calculado em todas as unidades de negócios, e um impacto global sobre toda a organização é, então, determinado. Quando há mescla de medidas qualitativas e quantitativas, a administração realiza uma avaliação qualitativa sobre as medidas de ambas, assim o resultado combinado é expresso em termos qualitativos. O estabelecimento de termos comuns de probabilidade e do grau de impacto por meio de toda a organização e categorias comuns de riscos para as medidas qualitativas facilita essas avaliações combinadas dos riscos.

Relação entre Eventos

Nos casos em que os eventos em potencial não estão relacionados, a administração os avaliará individualmente. Por exemplo, uma Companhia cujas unidades de negócios estão sujeitas a diferentes flutuações de preços – como polpa e moeda estrangeira – avaliaria os riscos separadamente quanto às flutuações de mercado. Porém quando existir alguma correlação entre os eventos, ou os eventos combinam-se e interagem para gerar probabilidades ou impactos significativamente diferentes, a administração os avaliará em conjunto. Enquanto que o impacto de um único evento pode ser moderado, o de uma seqüência ou combinação de eventos pode ser muito mais significativo.

Por exemplo, uma válvula defeituosa em um tanque de propano em um armazém de distribuição dá origem a um vazamento de propano; as portas do armazém são mantidas fechadas para evitar que o calor propague aos escritórios contíguos; o motorista de um caminhão que se aproxima e ativa um dispositivo de controle para abrir as portas do armazém. Juntas, a presença do gás propano e a faísca gerada pelo motor de acionamento da porta da garagem provocam uma explosão. Esses diferentes eventos interagem e produzem um impacto significativo. Em outro exemplo, uma Companhia ingressa em um mercado estrangeiro com gerentes recrutados localmente, sistemas de informação não testados e poucos dados para a administração central avaliar o seu desempenho com um risco significativo de demonstrativos errôneos ou fraudulentos.

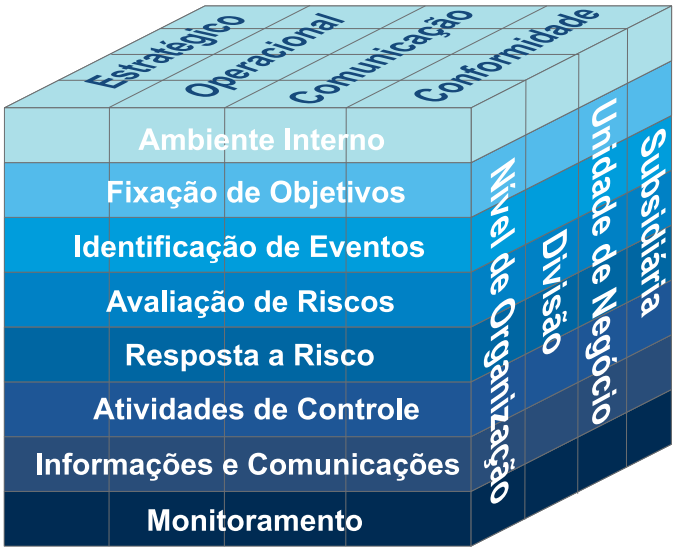
Nos casos em que os riscos podem afetar diversas unidades de negócios, a administração poderá agrupá-los em categorias de eventos e considerá-los primeiramente por unidade para, então, considerá-los em conjunto no âmbito de toda a organização. Por exemplo, as unidades de negócios de uma Companhia de serviços financeiros estão sujeitas a riscos de mudança das taxas de juros pagas pelo governo, e a sua administração avalia o risco não apenas em relação a cada uma das unidades de negócios, mas também o seu consolidado. Uma Companhia de manufatura possui diversas unidades de negócios, cada uma delas com exposição às flutuações no preço do ouro; a administração agrega o risco de alterações em potencial no preço do outro em uma única medida que mostra o efeito líquido da alteração de $1/onça em seu estoque total de ouro.

A natureza dos eventos e o fato de serem relacionados podem influenciar as técnicas de avaliação empregadas. Por exemplo, ao avaliar o impacto de eventos que podem provocar um impacto extremo, a administração poderá empregar o teste de estresse, enquanto que na avaliação dos efeitos de eventos múltiplos, a administração poderá considerar mais útil a análise de simulações ou de cenários.

O exame da relação entre a probabilidade e o impacto dos riscos representa uma importante responsabilidade gerencial. O gerenciamento de riscos corporativos eficaz requer que a avaliação de risco seja efetuada em relação aos riscos inerentes e, também, a resposta a riscos, conforme descreve o próximo capítulo.

6. Resposta a Riscos

Resumo do Capítulo: Após ter conduzido uma avaliação dos riscos pertinentes, a administração determina como responderá aos riscos. As respostas incluem evitar, reduzir, compartilhar ou aceitar os riscos. Ao considerar a própria resposta, a administração avalia o efeito sobre a probabilidade de ocorrência e o impacto do risco, assim como os custos e benefícios, selecionando, dessa forma, uma resposta que mantenha os riscos residuais dentro das tolerâncias a risco desejadas. A administração identifica as oportunidades que possam existir e obtêm, assim, uma visão dos riscos em toda organização ou de portfólio, determinando se os riscos residuais gerais são compatíveis com o apetite a riscos da organização.



As respostas a riscos classificam-se nas seguintes categorias:

- Evitar – Descontinuação das atividades que geram os riscos. Evitar riscos pode implicar a descontinuação de uma linha de produtos, o declínio da expansão em um novo mercado geográfico ou a venda de uma divisão.
- Reduzir – São adotadas medidas para reduzir a probabilidade ou o impacto dos riscos, ou, até mesmo, ambos. Tipicamente, esse procedimento abrange qualquer uma das centenas de decisões do negócio no dia-a-dia.
- Compartilhar – Redução da probabilidade ou do impacto dos riscos pela transferência ou pelo compartilhamento de uma porção do risco. As técnicas comuns compreendem a aquisição de produtos de seguro, a realização de transações de headging ou a terceirização de uma atividade.
- Aceitar – Nenhuma medida é adotada para afetar a probabilidade ou o grau de impacto dos riscos.

O Anexo 6.1 apresenta alguns exemplos de como se aplicam essas respostas a riscos.

Anexo 6.1

Evitar – Uma organização sem fins lucrativos identificou e avaliou os riscos de fornecer serviços médicos diretos aos seus membros e decidiu, desse modo, não aceitar os riscos associados. Além disso, a organização decidiu prestar um serviço de recomendação dos serviços.

Reduzir – Uma Companhia de compensação de títulos identificou e avaliou o risco de seus sistemas permanecerem inoperantes por um período superior a três horas e concluiu, assim, que não aceitaria o impacto dessa ocorrência. A Companhia investiu em tecnologia no aprimoramento de sistemas de auto-detecção de falhas e sistemas de back-up para reduzir a probabilidade de indisponibilidade do sistema.

Compartilhar – Uma universidade identificou e avaliou os riscos associados com a administração de seus dormitórios de estudantes e concluiu que não possuía internamente os requisitos necessários e as funcionalidades para administrar eficazmente essas grandes propriedades residenciais. A universidade terceirizou a administração do dormitório a uma empresa de administração de patrimônio, a fim de apresentar melhores condições de reduzir o impacto e a probabilidade de riscos relacionados com a propriedade.

Aceitar – Um órgão do governo identificou e avaliou os riscos de incêndio de sua infra-estrutura por meio de diversas regiões geográficas e o custo de compartilhar o impacto de seu risco mediante cobertura de seguro. O órgão concluiu que o custo adicional dos seguros e os dedutíveis associados ultrapassavam o custo provável de substituição e decidiram aceitar esse risco.

"Evitar" sugere que nenhuma opção de resposta tenha sido identificada para reduzir o impacto e a probabilidade a um nível aceitável. "Reduzir" ou "Compartilhar" reduzem o risco residual a um nível compatível com as tolerâncias desejadas ao risco, enquanto "Aceitar" indica que o risco inerente já esteja dentro das tolerâncias ao risco.

As opções adequadas de resposta são óbvias e bem aceitas em relação a muitos riscos. Por exemplo, para o risco de perder a disponibilidade de processamento de dados, uma opção típica de resposta seria a implementação de um plano de continuidade do negócio. Em relação a outros riscos, as opções disponíveis podem não estar muito aparentes, exigindo investigação e análise. Por exemplo, a identificação das opções de resposta pertinentes à redução do efeito das atividades da concorrência sobre o valor de marca poderá necessitar de pesquisa de mercado e análise.

Ao determinar respostas a riscos, a administração deverá levar em conta:

- os efeitos das respostas em potencial sobre a probabilidade e o impacto do risco – e que opções de resposta são compatíveis com as tolerâncias a risco da organização;
- os custos versus os benefícios das respostas em potencial;
- as possíveis oportunidades da organização alcançar seus objetivos vão além de se lidar com o risco específico

Para os riscos significativos, a organização tipicamente considera as respostas em potencial com base em um leque de opções de resposta. Esse procedimento possibilita maior profundidade à seleção das respostas e desafia o *status quo*.

Avaliação das Possíveis Respostas

Os riscos inerentes são analisados, e as respostas avaliadas com a finalidade de se alcançar um nível de risco residual compatível com as tolerâncias aos riscos da organização. Geralmente, qualquer uma das várias respostas compatibilizarão o risco residual com as tolerâncias ao risco, e, às vezes, uma combinação de respostas traz o melhor resultado. Por outro lado, às vezes, uma resposta afetará diversos riscos e nesse caso, a administração poderá decidir que não necessitará de medidas adicionais para abordar um determinado risco.

Avaliação do Efeito sobre a Probabilidade e Impacto do Risco

Na avaliação das opções de resposta, a administração considera o efeito da probabilidade e do impacto do risco, reconhecendo que uma determinada resposta poderá afetar, de forma diferente, a probabilidade e o impacto do risco. Por exemplo, uma organização cujo centro de processamento de dados localiza-se em uma região assolada por tempestades estabelece um plano de continuidade em outra localidade, a qual, apesar de não ter nenhum efeito sobre a probabilidade de ocorrência de tempestades, reduz o impacto dos danos às edificações ou de que o pessoal não consiga acesso ao local de trabalho. Por outro lado, a opção de transferir o centro de processamento de dados para outra região não reduzirá o impacto de uma tempestade da mesma intensidade, mas sim a probabilidade de ocorrência de tempestades no local da operação.

Ao analisar as respostas, a administração poderá considerar eventos e tendências anteriores, e o potencial de situações futuras. Via de regra, ao avaliar as respostas alternativas, a administração determina o seu efeito em potencial, utilizando as mesmas unidades de medida ou as compatíveis com as empregadas para o objetivo correspondente.

Avaliação de Custos versus Benefícios

Em razão das limitações de recursos, as organizações devem considerar os custos e os benefícios relativos às opções de respostas alternativas ao risco. As medições de custo-benefício para a implementação de respostas a riscos são realizadas com diversos níveis de precisão. De um modo geral, é mais fácil tratar do aspecto custo da equação, que, em muitos casos, pode ser quantificado com bastante precisão. Habitualmente, consideram-se todos os custos diretos associados ao estabelecimento de uma resposta, e os custos indiretos, caso sejam mensuráveis na prática. Algumas organizações também incluem os custos de oportunidade associados à utilização dos recursos.

Contudo, em alguns casos, é difícil quantificar os custos de resposta a riscos. Os problemas de quantificação surgem quando se estima o tempo e o esforço associados a uma determinada resposta, conforme o caso, como, na obtenção de inteligência de mercado a respeito da evolução das preferências dos clientes, em atividades da concorrência ou em outras informações geradas externamente.

O aspecto do benefício freqüentemente implica uma avaliação mais subjetiva. Por exemplo, os benefícios de programas eficazes de treinamento geralmente são aparentes, mas difíceis de se quantificar. Em muitos casos, entretanto, o benefício de uma resposta a risco pode ser avaliado no contexto do benefício associado com a realização do objetivo correspondente.

Por ocasião do exame das relações de custo-benefício, se a administração considerar os riscos como inter-relacionados, será possível agrupar as respostas de redução e de compartilhamento de riscos. Por exemplo, quando o risco é compartilhado por meio de seguro, pode ser vantajoso combiná-los em uma única apólice, pelo fato dos preços geralmente reduzirem-se quando as exposições combinadas são seguradas sob um único acordo financeiro.

Oportunidades nas Opções de Resposta

O capítulo de identificação de eventos descreve os métodos pelos quais a administração identifica eventos em potencial que podem afetar a realização de seus objetivos, positiva ou negativamente. Os eventos de impacto positivo representam oportunidades e são canalizados de volta para os processos de fixação de estratégias ou objetivos.

Da mesma forma, as oportunidades podem ser identificadas quando da resposta ao risco. As considerações de resposta a riscos não devem estar limitadas exclusivamente à redução de riscos identificados, mas devem considerar novas oportunidades para a organização. A administração poderá identificar respostas inovadoras, as quais, apesar de se encaixarem nas categorias de respostas descritas anteriormente neste capítulo, podem ser inteiramente novas para a organização ou para a indústria. Essas oportunidades podem emergir quando as opções de resposta a riscos atingem o limite da eficácia e quando refinamentos posteriores provavelmente possibilitarão apenas mudanças marginais ao impacto ou à probabilidade do risco. Pode-se citar o exemplo da resposta criativa de uma Companhia de seguros de automóveis ao elevado número de acidentes em certos cruzamentos. Essa Companhia decidiu financiar melhorias aos semáforos existentes, fato que reduziu os sinistros e melhorou suas margens operacionais.

Respostas Selecionadas

Uma vez avaliados os efeitos das respostas alternativas aos riscos, a administração decide como administrará o risco ao selecionar uma resposta ou combinação de respostas destinadas a trazer a probabilidade e o impacto do risco a parâmetros compatíveis de tolerância a riscos. A resposta não necessita gerar a quantidade mínima de risco residual. Mas quando uma resposta a risco gera um risco residual acima dos limites de tolerância, a administração retoma e reexamina a resposta ou, em certos casos, reconsidera os limites de tolerância estabelecidos em relação a esse risco. Desse modo, o processo de equilíbrio entre o risco e a tolerância a este pode implicar um processo iterativo.

A avaliação das respostas alternativas ao risco inerente requer considerar os riscos adicionais que podem ser gerados por uma resposta. Essa consideração também poderá originar um processo interativo pelo qual, antes de finalizar uma decisão, a administração leva em conta esses riscos adicionais, inclusive outros que não sejam evidentes imediatamente.

Assi que tiver selecionado uma resposta, a administração poderá necessitar desenvolver um plano de implementação para executá-la. Uma parte crítica do plano de implementação é o estabelecimento de atividades de controle (discutido no capítulo seguinte), para assegurar-se de que a resposta ao risco seja conduzida.

A administração reconhece que sempre existirá algum nível de risco residual, não somente porque os recursos são limitados, mas também em decorrência da incerteza e das limitações inerentes a todas as atividades empresariais.

Visão em Portfólio

O gerenciamento de riscos corporativos requer que o risco seja considerado a partir de uma perspectiva de toda a organização ou de portfólio. Geralmente, a administração adota uma abordagem na qual o risco é considerado, primeiramente, em relação a cada unidade de negócios, departamento ou função, em que o gerente responsável desenvolve uma avaliação combinada dos riscos para a unidade, refletindo o perfil de risco residual desta unidade em relação a seus objetivos e tolerâncias a riscos.

Tendo por base uma visão dos riscos em relação a unidades individuais, a alta administração de uma organização terá melhores condições de adotar uma visão de portfólio para determinar se o seu perfil de risco residual é compatível ao seu apetite a riscos relativo aos objetivos. Os riscos nas diferentes unidades podem estar dentro dos níveis de tolerância referentes a cada uma das unidades, mas, considerados em conjunto, os riscos poderão ultrapassar o apetite a risco da organização como um todo, em cujo caso será necessária uma resposta diferente ou adicional ao risco para compatibilizá-lo com o apetite a riscos. Por outro lado, os riscos podem equilibrar-se naturalmente na organização como um todo se, por exemplo, determinadas unidades individuais apresentam maior risco, enquanto outras são relativamente aversas a estes, de forma tal que o risco, em seu todo, seja compatível com o apetite a risco, eliminando-se assim a necessidade de uma resposta diferente a risco.

Uma visão de portfólio dos riscos pode ser apresentada nas formas mais variadas, como por exemplo, ao focalizar os principais riscos ou categorias de eventos por meio das unidades de negócios ou ao considerar a organização como um todo, utilizando medições como capital ajustado ao risco ou capital em risco. Essas medições compostas são particularmente úteis quando avalia o risco em relação aos objetivos definidos na forma de ganhos, crescimento ou outras medidas de desempenho, às vezes, relacionadas com o capital

alocado ou disponível. Essas medidas de visão de portfólio são capazes de fornecer informações úteis para redistribuir capital às unidades de negócios e para modificar o direcionamento estratégico.

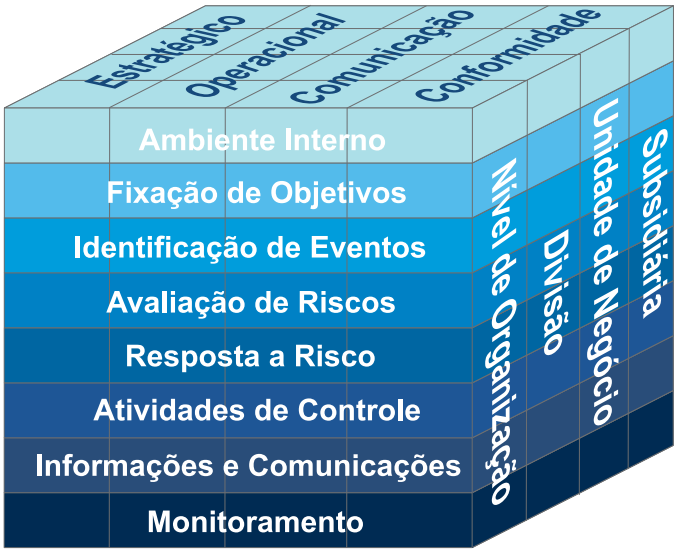
Temos o exemplo de uma Companhia de manufatura que adota uma visão de portfólio de risco cujo objetivo é a receita operacional. A administração utiliza categorias comuns de eventos para identificar riscos em suas unidades de negócios. Posteriormente, desenvolve um gráfico que apresenta, por categoria e por unidade de negócios, a probabilidade do risco em termos de freqüência em um período de tempo, bem como os relativos impactos sobre a receita. O resultado é uma visão composta ou de portfólio do risco que a Companhia enfrenta, e o conselho de administração e a diretoria executiva estão em condições de considerar não apenas a natureza, a probabilidade e o tamanho relativo dos riscos, mas também, como estes fatores podem afetar sua receita.

Outro exemplo é o de uma instituição financeira que visita as unidades de negócios para estabelecer objetivos, tolerâncias a riscos e medidas de desempenho, tudo em termos de retorno de capital ajustado ao risco. Esse tipo de medição, quando aplicado de forma consistente, possibilita à administração realizar as avaliações combinadas de risco das unidades na visão de portfólio de riscos para a instituição como um todo, permitindo que a administração considere os riscos das unidades por objetivos e determine se o apetite a riscos da instituição encontra-se em nível aceitável.

Ao examinar os riscos a partir de uma perspectiva de portfólio, a administração tem condições de verificar se a organização permanece nos limites de seu apetite a riscos. Além disso, poderá reavaliar a natureza e o tipo de risco que deseja assumir. Nos casos em que uma visão de portfólio apresente riscos significativamente menores do que o apetite a risco da organização, caberá à administração motivar os gerentes de cada unidade de negócio a assumir maior risco em áreas dirigidas, a fim de intensificar o crescimento e o retorno total.

7. Atividades de Controle

Resumo do capítulo: as atividades de controle são as políticas e os procedimentos que contribuem para assegurar que as respostas aos riscos sejam executadas. Essas atividades ocorrem em toda a organização, em todos os níveis e em todas as funções, pois compreendem uma série de atividades – tão diversas, como aprovação, autorização, verificação, reconciliação e revisão do desempenho operacional, da segurança dos bens e da segregação de responsabilidades.



As atividades de controle são políticas e procedimentos que direcionam as ações individuais na implementação das políticas de gestão de riscos, diretamente ou mediante a aplicação de tecnologia, a fim de assegurar que as respostas aos riscos sejam executadas. Essas atividades podem ser classificadas com base na natureza dos objetivos da organização aos quais os riscos de estratégia, operação, comunicação e cumprimento de diretrizes estão associados.

A despeito do fato de que algumas atividades de controle relacionam-se exclusivamente com uma categoria, sempre haverá alguma sobreposição. Dependendo das circunstâncias, uma determinada atividade de controle pode ajudar a atender aos objetivos da organização em mais de uma categoria. Por exemplo, esses controles também podem assegurar relatórios confiáveis, que, por sua vez, podem servir para assegurar o seu cumprimento e assim por diante.

Integração com Resposta a Riscos

Ao selecionar as respostas aos riscos, a administração identifica as atividades de controle necessárias para assegurar que estas sejam executadas de forma adequada e oportuna.

A associação de objetivos, respostas a riscos e atividades de controle é ilustrada no exemplo a seguir: uma Companhia estabelece como objetivo alcançar ou exceder as metas de vendas, identificando como risco a falta de conhecimentos suficientes de fatores externos sejam as necessidades atuais do cliente sejam as em potencial. Para reduzir a probabilidade da ocorrência e do impacto do risco, a administração recorre aos históricos de compras dos clientes existentes e empreende novas iniciativas de pesquisa de mercado. Essas respostas a riscos servem de referência para estabelecer atividades de controle, e, também, acompanhar o progresso e o desenvolvimento do histórico de compras de cliente em relação às programações estabelecidas e à adoção de medidas para assegurar a precisão dos dados relatados. Sendo assim, as atividades de controle são diretamente inseridas no processo de administração.

Ao selecionar as atividades de controle, a administração considera a forma como essas atividades se relacionam entre si. Em alguns casos, uma única atividade de controle aborda diversas respostas a riscos. Em outros, diversas atividades de controle são necessárias para apenas uma resposta a risco. E, ainda, em outras situações, a administração poderá constatar que as atividades de controle existentes são suficientes para assegurar a execução eficaz das novas respostas a riscos.

Embora as atividades de controle geralmente sejam estabelecidas para assegurar que as respostas aos riscos sejam bem executadas em relação a determinados objetivos, as próprias atividades de controle são respostas a riscos. Por exemplo, para que um objetivo assegure que determinadas transações tenham sido devidamente autorizadas, a resposta provavelmente será na forma de atividades de controle, como a diferenciação de deveres e a aprovação pelo pessoal de supervisão.

Da mesma forma que a seleção de respostas a riscos considera a adequação e os riscos remanescentes ou residuais, a seleção ou a revisão das atividades de controle deve avaliar a pertinência e a adequação aos objetivos correspondentes. Isso pode ser alcançado considerando separadamente da adequação das atividades de controle, ou, considerando o risco residual nos contextos tanto da resposta ao risco quanto das atividades de controle correspondentes.

As atividades de controle são importantes elementos do processo por meio do qual uma organização busca atingir os objetivos do negócio. Elas não são executadas simplesmente por executar ou por parecer a coisa “certa ou apropriada” a ser feita. No exemplo acima, a administração necessita adotar medidas para assegurar que as metas de vendas sejam alcançadas. As atividades de controle servem como mecanismos de gestão do cumprimento desse objetivo.

Tipos de Atividades de Controle

Existe uma variedade de descrições distintas quanto aos tipos de atividades de controle, inclusive as preventivas, as detectivas, as manuais, as computadorizadas e as de controles administrativos. Essas atividades também podem ser classificadas com base nos objetivos de controle especificados, como o de assegurar a integridade e a precisão do processamento de dados.

O Anexo 7.1, a seguir; descreve as atividades de controle geralmente utilizadas, as quais representam apenas uma parcela dos muitos procedimentos comumente executados pelo pessoal em vários níveis organizacionais. A meta dessas atividades é reforçar o cumprimento de planos de ação estabelecidos e, também, manter as organizações direcionadas ao cumprimento de seus objetivos. Elas estão apresentadas apenas para ilustrar a gama e a variedade de atividades de controle, não para sugerir qualquer classificação especial.

Anexo 7.1

- Revisões da Alta Direção – a alta direção compara o desempenho atual em relação ao orçado, às previsões, aos períodos anteriores e aos de concorrentes. As principais iniciativas são acompanhadas, como campanhas de marketing, processos de melhoria de produção e programas de contenção ou de redução de custo, para medir até que ponto as metas estão sendo alcançadas. A implementação de planos é monitorada no caso de desenvolvimento de novos produtos, join ventures ou novos financiamentos.
- Administração Funcional Direta ou de Atividade – gerentes, no exercício de suas funções ou atividades examinam relatórios de desempenho. Um gerente responsável pelos empréstimos bancários a consumidores revisa os relatórios por filial, região e tipo de empréstimo (com caução), verificando resumos e identificando tendências e associando os resultados a estatísticas econômicas e metas. Por sua vez, os gerentes de filiais também se concentram em questões de cumprimento de políticas, revisando relatórios exigidos por órgãos reguladores a respeito de novos depósitos acima de um determinado valor. São realizadas reconciliações dos fluxos de caixa diários, com as posições líquidas relatadas centralmente para transferências e investimentos no *overnight*.
- Processamento da Informação – uma variedade de controles é realizada para verificar a precisão, a integridade e a autorização das transações. Os dados inseridos ficam sujeitos a verificações de edição on-line ou à combinação com arquivos aprovados de controle. Um pedido de cliente, por exemplo, somente poderá ser aceito após fazer referência a um arquivo de cliente e ao limite de crédito aprovado. As seqüências numéricas das transações são levadas em conta, sendo as exceções acompanhadas e relatadas aos supervisores. O desenvolvimento de novos sistemas e as mudanças nos já existentes são controlados da mesma forma que o acesso a dados, arquivos e programas.
- Controles Físicos – os equipamentos, estoques, títulos, dinheiro e outros bens são protegidos fisicamente, contados periodicamente e comparados com os valores apresentados nos registros de controle.
- Indicadores de Desempenho – relacionar diferentes conjuntos de dados, sejam eles operacionais sejam financeiros, em conjunto com a realização de análises dos relacionamentos e das medidas de investigação e correção, funciona como uma atividade de controle. Os indicadores de

desempenho incluem, por exemplo, índices de rotação de pessoal por unidade. Ao investigar resultados inesperados ou tendências incomuns, a administração poderá identificar circunstâncias nas quais a falta de capacidade para concluir processos fundamentais pode significar menor probabilidade dos objetivos serem alcançados. A forma como a administração utiliza essas informações – somente no caso de decisões operacionais ou, também, no caso do acompanhamento de resultados imprevistos nos sistemas de comunicações – determinará se a análise dos indicadores de desempenho por si só atenderá às finalidades operacionais, bem como às finalidades de controle da comunicação.

- Segregação de funções – as obrigações são atribuídas ou divididas entre pessoas diferentes com a finalidade de reduzir o risco de erro ou de fraude. Por exemplo, as responsabilidades de autorização de transações, do registro ed a entrega do bem em questão são divididas. O gerente que autoriza vendas a crédito não deve ser responsável por manter os registros de contas a pagar nem pela distribuição de recibos de pagamentos. Da mesma forma, os vendedores não devem modificar arquivos de preços de produtos nem as taxas de comissão.

Geralmente, implementa-se uma combinação de controles para tratar das respostas relacionadas a riscos. A administração de uma Companhia, por exemplo, estabelece limites para transações, a fim de administrar os riscos relacionados com um dado portfólio de investimentos, e cria atividades de controle específicas para assegurar que os limites das transações não sejam ultrapassados. As atividades de controle incluem os preventivos, que evitam a concretização de determinadas transações, e os de detecção, que identificam outras transações discrepantes oportunamente. Essas atividades combinam controles informatizados e manuais, inclusive os controles automatizados, para assegurar que todas as informações sejam colhidas corretamente e que os procedimentos de rotina permitam que os indivíduos responsáveis autorizem ou aprovem as decisões de investimentos.

Políticas e Procedimentos

De modo geral, as atividades de controle incluem dois elementos: uma política que estabelece aquilo que deverá ser feito e os procedimentos para fazê-la ser cumprida. Por exemplo, uma política poderá requerer a revisão das atividades de negociação do cliente pelo gerente de varejo da filial com a corretora. O procedimento é a própria revisão, realizada oportunamente e com especial atenção para os fatores estabelecidos na política, como a natureza e o volume dos títulos transacionados e o volume destes em relação ao patrimônio líquido e à idade do cliente.

Muitas vezes, as políticas são comunicadas verbalmente. As que não são escritas podem ser eficazes quando existem há muito tempo e são adequadamente entendidas, e nas pequenas organizações em que os canais de comunicação envolvem poucas camadas gerenciais e existe uma estreita interação e supervisão dos empregados. No entanto, independentemente do fato de estar escrita ou não, uma política deve ser implementada com atenção, de forma conscienciosa e consistente. Um procedimento não terá nenhuma utilidade se for executado mecanicamente, sem um enfoque nítido e contínuo nas condições às quais a política se destina. Além disso, é essencial que as condições identificadas em razão do procedimento sejam analisadas e que medidas corretivas apropriadas sejam adotadas. As medidas de acompanhamento podem variar com base no tamanho e na estrutura organizacional da organização e podem percorrer os processos formais de comunicação, como no caso de uma Companhia de grande porte – em que as unidades comerciais relatam o motivo pelo qual suas metas não foram alcançadas e quais as medidas adotadas para evitar a repetição do evento ou como no caso de um proprietário-diretor de uma pequena empresa, que atravessa o corredor para falar com o gerente de fábrica sobre o que deu errado e o que necessita ser feito.

Controles dos Sistemas de Informações

A dependência cada vez maior em relação a sistemas de informações para auxiliar a operação de uma organização e para atender aos objetivos de comunicação e ao cumprimento de políticas traz a necessidade de controle dos sistemas mais significativos. Dois grupos amplos de atividades de controle dos sistemas de informação podem ser utilizados. O primeiro diz respeito aos controles gerais, que se aplicam a praticamente todos os sistemas e contribuem para assegurar uma operação adequada e contínua. O segundo grupo é o dos controles de aplicativos, que incluem etapas para avaliar o processo por meio de códigos de programação dentro do software. Os controles gerais e os de aplicativos, em conjunto com os processos de controle manual, quando necessários, asseguram a integridade, a precisão e a validade das informações.

Controles Gerais

Os controles gerais estendem-se pela administração da tecnologia da informação, pela infra-estrutura da tecnologia da informação, pela administração da segurança, pela aquisição de software, pelo desenvolvimento e pela manutenção. Esses controles aplicam-se a todos os sistemas: os de grande porte ou mainframe para cliente/servidor aos ambientes de computadores portáteis e os de mesa. O Anexo 7.2 apresenta alguns exemplos de controles comuns nessas categorias.

Anexo 7.2

- Administração da Tecnologia da Informática – um comitê diretivo supervisiona, monitora e relata as atividades da tecnologia da informática e as iniciativas de melhoria.

- Infra-estrutura da Tecnologia da Informática – os controles são aplicados para definir, adquirir, instalar, configurar, integrar e fazer a manutenção de sistemas. Os controles podem incluir acordos de níveis de serviço que estabelecem e reforçam o desempenho do sistema, planejamento da continuidade dos negócios que mantém a disponibilidade do sistema e, também, acompanhamento do desempenho da rede, no caso de falhas operacionais e da programação das operações de informática. O software do sistema, componente da infra-estrutura da tecnologia da informação, pode incluir controles da parte da administração e do comitê diretivo, como revisão e aprovação de novas aquisições significativas, limitação do acesso à configuração do sistema e operação do software de sistema, reconciliações automatizadas dos dados acessados por meio de software intermediário e detecção de paridade por bit para a comunicação de erros. Os controles de software do sistema também incluem o monitoramento de incidentes, *logging* de sistema e revisão dos relatórios, detalhando a utilização de utilitários para alteração de dados.

- Administração da Segurança – controles lógicos de acesso como as senhas de segurança à rede, à base de dados e aos aplicativos. Contas de usuários e controles relacionados de privilégios de acesso contribuem para limitar os usuários autorizados a utilizar apenas os aplicativos ou funções de aplicativos necessárias ao cumprimento de suas tarefas. Firewalls da Internet e redes virtuais particulares protegem os dados contra acesso externo não autorizado.

- Aquisição, Desenvolvimento e Manutenção de Software – os controles de aquisição e de implementação de software estão incorporados em um processo estabelecido para administrar mudanças, inclusive os requisitos de documentação, o teste de aceitação pelo usuário e as avaliações de riscos do projeto. O acesso a códigos-fonte é controlado por meio de uma biblioteca de códigos. Os programadores de software trabalham somente em ambientes isolados de desenvolvimento/teste e não têm acesso ao ambiente da produção. Os controles de mudanças de sistema incluem a obrigatoriedade de autorização para solicitar as mudanças, a revisão das mudanças, as aprovações, a documentação, o teste, as implicações das mudanças para outros componentes da tecnologia da informática, os resultados de testes de estresse e os protocolos de implementação.

Controle de Aplicativos

Os controles de aplicativos concentram-se diretamente na configuração, precisão, autorização e validação da coleta e do processamento de dados. Esses controles ajudam a assegurar que os dados sejam colhidos ou gerados quando houver necessidade, quando os aplicativos de apoio estiverem disponíveis e quando os erros de interface forem detectados prontamente.

Um objetivo importante dos controles de aplicativos é evitar a possibilidade de erros no sistema, além de detectar e corrigir os que estiverem presentes. Para isso, esses controles comumente utilizam verificações de edição, que consistem em verificar o formato, a existência, a razoabilidade e permitam verificar dados construídos nos aplicativos durante a sua fase de desenvolvimento. Se formulados adequadamente, podem possibilitar o controle dos dados que entram no sistema.

O Anexo 7.3 apresenta exemplos de controles de aplicativos. Esses controles são apenas alguns de uma ampla série de controles realizados todos os dias, mediante cálculos e comparações que servem para evitar e detectar a coleta e o processamento incompleto, inexato, inconsistente e inadequado de dados.

Anexo 7.3

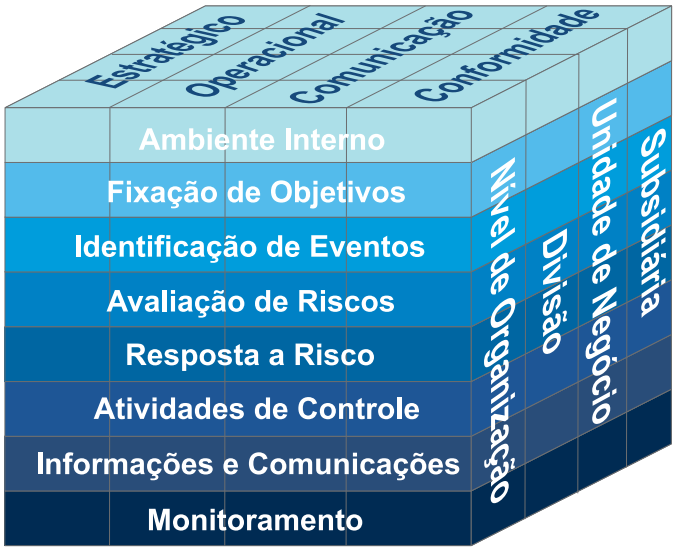
- Balanço das Atividades de Controle – detecta erros de captura de dados por meio da reconciliação da quantidade imputada manual ou automaticamente em relação ao total controlado. Uma Companhia faz o balanço automático entre a quantidade total de transações processadas e lançadas no seu sistema de entrada de pedidos on-line e a quantidade de transações recebidas em seu sistema de faturamento.
- Dígitos de Verificação – validam os dados por meio de cálculos. É gerado à partir do código da organização, um dígito de verificação para detectar e corrigir pedidos imprecisos de seus fornecedores.
- Listagens Predefinidas de Dados – fornecem aos usuários listagens predefinidas de dados aceitáveis. O site de intranet de uma organização inclui listas suspensas dos produtos oferecidos para venda.
- Testes da Razoabilidade de Dados – comparam os dados colhidos com um padrão atual ou aprendido de razoabilidade. Um pedido a fornecedor de uma loja de material de construção de varejo solicitando uma quantidade excessiva de metros cúbicos de madeira será identificado na comparação de razoabilidade e irá requerer uma revisão.
- Testes Lógicos – incluem a utilização de limites de faixas ou de valor ou testes alfanuméricos. Um órgão do governo constata erros em potencial em número do seguro social ao verificar se todos os números digitados contêm nove dígitos.

Específicos da Organização

Pelo fato de cada organização ter seu próprio conjunto de objetivos e abordagens de implementação, sempre haverá diferenças nas respostas a riscos e nas atividades de controle relacionadas. Ainda que duas organizações com objetivos idênticos tomem decisões semelhantes sobre o modo de atingir os seus objetivos, é provável que as atividades de controle sejam diferentes. As organizações, por serem administradas por pessoas diferentes, utilizam critérios próprios para exercer o controle. Além disso, os controles refletem o ambiente e a indústria nos quais a organização opera, bem como o porte e a complexidade, a natureza e o alcance de suas atividades, sua história e sua cultura.

As organizações de grande porte e mais complexas, com diversas atividades, podem enfrentar questões de controle mais difíceis do que organizações pequenas, simples com atividades menos variadas. Uma Companhia de operações descentralizadas, que ressalte a autonomia local e a inovação, apresentará características de controle distintas de outra altamente centralizada. Entre os outros fatores que podem influenciar o grau de complexidade da organização e, portanto, a natureza de seus controles estão a localização e a dispersão geográfica, o tamanho e o grau de sofisticação das operações, bem como os métodos de processamento das informações.

8. Informação e Comunicação



Resumo do capítulo: as informações pertinentes são identificadas, coletadas e comunicadas de forma coerente e no prazo, a fim de permitir que as pessoas cumpram as suas responsabilidades. Os sistemas de informática geralmente empregam dados gerados internamente e informações de fontes externas, possibilitando, dessa forma, esclarecimentos para o gerenciamento de riscos e tomada de decisão baseadas em dados relacionados aos objetivos. A comunicação eficaz também ocorre ao fluir em todos os níveis da organização. Todo o pessoal recebe uma mensagem clara da alta administração, alertando que as responsabilidades do gerenciamento de riscos corporativos devem ser levadas a sério. Cada um entende a sua própria função no gerenciamento de riscos corporativos, assim como as atividades individuais que se relacionam com o trabalho dos demais. As pessoas deverão ter uma forma de comunicar informações significativas dos escalões inferiores aos superiores. Deve haver, também, uma comunicação eficaz com terceiros, como clientes, fornecedores, órgãos reguladores e acionistas.

Toda organização identifica e coleta uma ampla gama de informações relacionadas a atividades e eventos externos e internos, pertinentes à administração. Essas informações são transmitidas ao pessoal em uma forma e um prazo que lhes permita desempenhar suas responsabilidades na administração de riscos corporativos e outras.

Informações

As informações são necessárias em todos os níveis de uma organização, para identificar, avaliar e responder a riscos, administrá-la e alcançar seus objetivos. Uma ampla série de informações é utilizada, pertinente a uma ou mais categorias de objetivos.

As informações operacionais de fontes internas e externas, de natureza financeira e não-financeira, são relevantes a diversos objetivos comerciais. As informações financeiras, por exemplo, são empregadas no desenvolvimento de demonstrações financeiras para fins de comunicação e decisões operacionais como o monitoramento do desempenho e da alocação de recursos. As informações financeiras confiáveis são fundamentais ao planejamento, à elaboração de orçamentos, à fixação de preços, às avaliações do desempenho de vendedores, à avaliação de empreendimentos conjuntos e alianças, bem como uma faixa de outras atividades gerenciais.

Da mesma forma, as informações operacionais são essenciais ao desenvolvimento de relatórios financeiros e outros, entre eles as transações rotineiras de compras, vendas e outras, além de informações em relação ao lançamento de produtos da concorrência ou de suas condições econômicas, as quais podem influenciar avaliações de estoques e de contas a receber. E as informações necessárias para fins de conformidade, como dados relacionados à emissão de poluentes na atmosfera ou dados dos empregados, também podem atender aos objetivos dos relatórios financeiros.

As informações originam-se de muitas fontes – internas e externas, e nas formas quantitativas e qualitativas – e facilitam as respostas às condições alteradas. Um dos desafios que se apresenta à administração é o processamento e a depuração de grandes volumes de dados em informações úteis. Esse processo analisa e relata as informações relevantes. Esses sistemas de informações – geralmente informatizados, mas que se utilizam de entradas ou interfaces manuais – comumente são considerados no contexto do processamento de dados gerados internamente. Porém os sistemas de informações possuem uma aplicação muito mais ampla. Esses sistemas também tratam de informações referentes a eventos internos e externos, por exemplo, dados econômicos específicos a um mercado ou uma indústria que apontam para mudanças na demanda dos produtos ou serviços de uma Companhia, dados de bens e serviços para processos de produção, informações de inteligência de mercado sobre mudanças nas preferências ou exigências de consumidores, informações relacionadas às atividades de desenvolvimento de produtos da concorrência e iniciativas legislativas ou reguladoras.

Os sistemas de informações podem ser formais ou informais. Conversas com clientes, fornecedores, órgãos reguladores e empregados da organização freqüentemente provêm informações críticas necessárias à identificação de riscos e de oportunidades. Da mesma forma, a participação em seminários de profissionais ou da indústria, bem como o ingresso em associações comerciais e outras podem ser fontes valiosas de informações.

É, particularmente, importante manter as informações compatíveis com as necessidades, quando uma Companhia enfrenta mudanças fundamentais no setor, concorrentes altamente inovadores e rápidos ou mudanças significativas na demanda dos clientes. Os sistemas de informações modificam-se conforme necessário para o suporte de novos objetivos. Eles identificam e capturam as informações necessárias, financeiras e não-financeiras, processando e relatando-as na forma e no tempo que as torne úteis ao controle da atividade da empresa.

Sistemas Estratégicos e Integrados

Na medida em que as Companhias tornam-se mais colaborativas e integradas com clientes, fornecedores e parceiros de negócio, a divisão entre a arquitetura dos sistemas de informações de uma organização e a de terceiros torna-se cada vez menos nítida. Conseqüentemente, o processamento e a administração de dados, geralmente, tornam-se uma responsabilidade compartilhada por diversas organizações. Nesses casos, a arquitetura dos sistemas de informações de uma organização deve ser suficientemente flexível e ágil para integrar-se de forma efetiva às partes externas relacionadas.

O desenho da arquitetura de um sistema de informações e a aquisição de tecnologia são aspectos importantes da estratégia de uma organização, e as opções em relação à tecnologia podem ser críticas à realização dos objetivos. As decisões referentes à escolha e à implementação da tecnologia dependem de inúmeros fatores, inclusive de metas organizacionais, necessidades de mercado e requisitos competitivos. Embora os sistemas de informações sejam fundamentais ao eficaz gerenciamento dos riscos corporativos, o próprio uso de técnicas de gestão de riscos pode ajudar nas decisões tecnológicas.

Desde há muito, os sistemas de informações foram projetados e utilizados para fornecer suporte à estratégia comercial. Essa função torna-se crítica à medida que as necessidades do negócio modificam-se, e a tecnologia cria novas oportunidades de explorar vantagens estratégicas. Em alguns casos, as mudanças na tecnologia reduziram a vantagem obtida na alocação inicial de recursos, dando lugar a um novo direcionamento estratégico. Por exemplo, os sistemas de reservas de Companhias aéreas, que possibilitam aos agentes de viagens um fácil acesso às informações de vôo, posteriormente, deslocaram-se para sistemas de reservas pela Internet com acesso do cliente, reduzindo significativamente ou até eliminando a figura do agente de viagens tradicional.

Integração com Operações

Freqüentemente, os sistemas de informações estão totalmente integrados à maioria dos aspectos das operações. Os sistemas da Internet ou com base nela são comuns, com muitas organizações oferecendo sistemas de informações de toda a organização, como o planejamento de recursos. Esses aplicativos facilitam o acesso às informações – que anteriormente ficavam retidas nos silos funcionais ou nos departamentos – e as disponibilizam para um uso amplo pela administração. As transações são registradas e rastreadas em tempo real, permitindo aos gestores acesso imediato e mais eficaz a informações financeiras e operacionais para o controle das atividades comerciais. Por exemplo, uma Companhia de construção civil que atua em diversos projetos de grande escala emprega um sistema integrado, com base na Extranet para alcançar às expectativas de eficiência e dos mercados. O sistema provê informações que auxiliam o gestor a acompanhar o estoque e as peças fornecidas ao cliente, identificar materiais em excesso ou em falta em diversos locais, obter economias de custo com os fornecedores de materiais comuns ou, ainda, aliar-se a organizações semelhantes para obter descontos de volume, bem como monitorar as atividades dos sub empreiteiros. O sistema também permite que os empregados compartilhem exatamente as plantas atuais com os arquitetos, engenheiros, clientes, sub empreiteiros e órgãos normativos, bem como, ao mesmo tempo, manter o controle da versão da planta. Além disso, o sistema abrange funcionalidades de gestão de conhecimentos que permitem aos empregados compartilhar soluções inovadoras por toda a organização.

Para fornecer suporte eficaz à administração de riscos corporativos, a organização coleta e utiliza dados históricos e correntes. Os dados históricos permitem que a organização acompanhe o desempenho real em relação às metas, aos planos e às expectativas. Esses dados possibilitam *insights* sobre o seu desempenho nas mais diversas condições, permitindo que a administração identifique correlações e tendências, bem como faça previsões em relação ao desempenho futuro. Os dados históricos também possibilitam um aviso antecipado dos eventos em potencial que merecem a atenção da administração.

Os dados atuais ou da situação corrente permite que uma organização determine se está ou não dentro das tolerâncias estabelecidas para riscos. Esses dados possibilitam aos gestores uma visão em tempo real dos riscos existentes em um processo, uma função ou uma unidade e a identificação de variações em relação às expectativas.

Para muitas organizações, o desenvolvimento dos sistemas de informação melhora a capacidade de mensurar e monitorar o desempenho, bem como apresentar informações analíticas no âmbito de toda a organização. A complexidade dos sistemas e a integração continuam com as organizações ao utilizar as novas funcionalidades da tecnologia na medida em que surgem. Contudo, a crescente dependência em relação aos sistemas de informações nos níveis estratégico e operacional gera novos riscos – como a violação da segurança de informações ou crimes cibernéticos – que necessitam ser integrados à administração de riscos.

Profundidade e Pontualidade das Informações

A infra-estrutura de informações obtém e colhe os dados de acordo com uma programação e a profundidade consistentes com a necessidade que a organização tem de avaliar, responder a riscos e permanecer dentro de suas tolerâncias a riscos. A pontualidade do fluxo de informações necessita ser consistente com o índice de mudança dos ambientes interno e externo.

A importância da profundidade dos dados é ilustrada, considerando-se os eventos diferentes que afetam uma corretora de seguros situada em uma cidade sujeita a inundações. Como parte de seu planejamento da continuidade dos negócios, a administração mantém uma percepção generalizada das condições de inundação em potencial e posiciona-se para orientar o pessoal quando devem se mudar para as instalações de emergência. As informações colhidas nesse nível elevado são suficientes para permitir que a corretora administre o risco de forma adequada. Por outro lado, na condição de corretora, a empresa busca e coleta continuamente as alterações nos preços das ações, das obrigações e das *commodities* até várias casas decimais. Esse nível de pontualidade e de detalhe de dados é consistente com a necessidade que a corretora tem de responder imediatamente a mudanças de preços que podem desencadear riscos, como excesso de exposição a um determinado setor ou segurança de mercado de forma inconsistente com o apetite a riscos.

A infra-estrutura de informações converte dados em informações pertinentes que ajudarão os funcionários a conduzir o gerenciamento de riscos corporativos e outras responsabilidades. As informações são fornecidas em uma programação e forma que possa ser acessada, prontamente utilizada e associada a determinadas responsabilidades.

Avanços na coleta, no processamento e no armazenamento de dados provocaram um crescimento exponencial no volume de dados. Contando com mais dados disponíveis – geralmente em tempo real – para um maior número de pessoas em uma organização, o desafio será evitar “sobrecarga de informações” assegurando-se um fluxo para as informações corretas, na forma correta, no nível correto de detalhes, para as pessoas certas, na ocasião oportuna. Ao desenvolver a infra-estrutura de conhecimento e de informações, devem-se considerar os diferentes requisitos de informações de cada usuário e departamento individual, bem como resumir no nível estipulado as informações que necessitam os diferentes níveis de gestão.

Qualidade das Informações

Em face da crescente dependência em relação a sistemas sofisticados de informações e sistemas e processos automatizados de decisão, acionados por dados, a confiabilidade dos dados é um fator crítico. Dados imprecisos podem gerar riscos não identificados ou avaliações deficientes e decisões gerenciais inadequadas.

A qualidade das informações implica verificar se:

- O conteúdo é apropriado – está no nível de detalhes adequado?
- As informações são oportunas – estarão disponíveis quando necessário?
- As informações são atuais – são as mais recentes?
- As informações são exatas – os dados estão corretos?
- As informações são de fácil acesso – são de fácil obtenção por aqueles que as necessitam?

Para aprimorar a qualidade dos dados, as organizações estabelecem programas de gerenciamento de dados do âmbito de toda a organização, abrangendo a aquisição, a manutenção e a distribuição de informações relevantes. Sem esses programas, os sistemas de informações não seriam capazes de fornecer as informações que a administração e outros empregados venham a necessitar.

São muitos os desafios: necessidades funcionais conflitantes, limitações de sistema e processos não integrados podem inibir a aquisição de dados e o uso eficaz. Para atender a esses desafios, a administração estabelece um plano estratégico com clara definição de responsabilidades pela integridade dos dados e executa avaliações periódicas da qualidade dos dados.

De posse das informações corretas oportunamente e no local adequado, é essencial conduzir o gerenciamento de riscos corporativos. Por esse motivo, os sistemas de informações, apesar de serem um componente do gerenciamento de riscos corporativos, devem também ser controlados.

Comunicações

A comunicação é inerente a todos os sistemas de informações. Como já discutimos acima, os sistemas de informações devem fornecer informações ao pessoal apropriado para que este possa desincumbir-se de suas responsabilidades operacionais, de comunicação e de conformidade. Porém a comunicação também deve ocorrer em um sentido mais amplo, tratando de expectativas, responsabilidades de indivíduos e grupos, bem como outras questões importantes.

Internas

A administração fornece comunicações específicas e dirigidas que abordam as expectativas de comportamento e as responsabilidades do pessoal. Isso inclui uma clara definição da filosofia e da abordagem do gerenciamento de riscos corporativos, além de uma clara delegação de autoridade. A comunicação referente aos processos e aos procedimentos deverá alinhar-se e apoiar a cultura desejada.

As comunicações devem transmitir com eficácia:

- a importância e a pertinência do gerenciamento de riscos corporativos eficaz;
- os objetivos da organização;
- o apetite a riscos e a respectiva tolerância;
- uma linguagem comum de riscos;
- as funções e as responsabilidades do pessoal ao conduzir e apoiar os componentes do gerenciamento de riscos corporativos.

Todos os empregados, especialmente os indivíduos aos quais foram atribuídas importantes responsabilidades de gestão operacional ou financeira, necessitam receber uma mensagem clara da alta administração alertando que o gerenciamento de riscos corporativos deve ser levado a sério. Tanto a clareza da mensagem e a eficácia com a qual é comunicada são fatores importantes.

O pessoal também necessita saber de que forma as suas atividades relacionam-se com o trabalho dos outros. Esse conhecimento é necessário para reconhecer um problema, determinar a sua causa e definir uma medida corretiva. Além disso, necessitam saber o que é considerado comportamento aceitável e inaceitável. Já tivemos a oportunidade de ver exemplos famosos de relatórios fraudulentos nos quais os gestores que, pressionados para observar orçamentos, mascararam resultados operacionais. Em diversos casos, ninguém havia dito ao pessoal envolvido que esses relatos enganosos eram ilegais ou até impróprios. Esses casos ressaltam a natureza crítica da forma pela qual as mensagens são comunicadas em uma organização. Um gestor que instrui seus subordinados a “respeitar o orçamento, sem importar-se com o que poderá acontecer” poderá estar, inconscientemente, enviando-lhes uma mensagem equivocada.

Os empregados da linha de frente que tratam questões operacionais críticas todos os dias, geralmente, têm melhor condição de reconhecer problemas na medida em que surgem. Assim, cabe aos canais de comunicação assegurar que o pessoal é capaz de comunicar informações baseadas em riscos por todas as unidades comerciais, os processos ou os silos funcionais e para os seus superiores. Por exemplo, representantes de vendas ou gerentes de contas podem conhecer necessidades importantes de design de produto do cliente, o pessoal da produção pode constatar deficiências custosas de processo, e o pessoal de compras pode se deparar com

incentivos indevidos de fornecedores. As falhas de comunicação podem ocorrer quando pessoas ou unidades perdem a motivação de fornecer informações importantes a outras pessoas ou não dispõem de um meio de fazê-lo. O pessoal pode estar ciente de riscos significativos, mas não se mostrar disposto nem capaz de relatá-los.

Para que essas informações possam ser relatadas, deverá haver canais de comunicação abertos e uma nítida disposição de ouvi-los. O pessoal deve acreditar que os seus superiores realmente desejam conhecer os problemas tratando-os, desse modo, com eficácia. Quase todos os gestores reconhecem intelectualmente que devem evitar "atirar no mensageiro." Porém, quando envolvidos nas pressões do dia-a-dia, podem não se mostrar muito receptivos a pessoas que lhes tragam problemas verdadeiros. Os empregados aprendem rapidamente a identificar os sinais de que um superior não tem tempo ou interesse de tratar dos problemas que constataram. Para piorar ainda mais a situação, o gestor não receptivo é sempre o último a saber que o canal de comunicação foi efetivamente desativado.

Na maioria dos casos, as linhas normais de comunicação em uma organização representam os canais adequados. Contudo, em determinadas circunstâncias, são necessárias linhas separadas de comunicação, que servirão de proteção contra falhas, caso os canais normais apresentem-se inoperantes. Muitas organizações estabelecem e fazem os empregados saber de um canal direto com o auditor interno chefe ou consultor jurídico ou outro empregado de alto escalão que tenha acesso à diretoria executiva, com o processo de supervisão pelo conselho de administração ou pelo comitê de auditoria. Além disso, leis e regulamentos solicitam cada vez mais que as organizações estabeleçam esses mecanismos. Em razão de sua importância, o gerenciamento de riscos corporativos eficaz requer esse tipo de canal de comunicação. Sem esses canais e a disposição de ouvir, o fluxo ascendente de informações poderá bloquear-se.

É importante que o pessoal entenda que não haverá represália para o relato de informações relevantes. Uma mensagem clara é transmitida pela simples existência de mecanismos que incentivem os empregados a relatar suspeitas de violação de qualquer um dos códigos de conduta da organização e pelo tratamento que será dado a quem apresentar a denúncia.

Um código de conduta detalhado e pertinente, sessões de informação aos empregados, comunicações corporativas contínuas e mecanismos de *feedback* com o exemplo correto dado mediante os atos da alta administração poderão reforçar essas importantes mensagens.

O canal entre a alta administração e a diretoria executiva é um dos mais críticos canais de comunicação. A administração deve manter a diretoria executiva atualizada em relação ao desempenho, ao risco e ao funcionamento do gerenciamento de riscos corporativos e a outros eventos e questões importantes. Quanto melhor a comunicação, maior eficácia terá a diretoria no desempenho de sua função de supervisão - fazendo as vezes de um "conselho sonoro" para a administração em relação a questões críticas, monitorando, dessa forma, as atividades e fornecendo orientação, assessoria e direção. Por outro lado, a diretoria deverá informar as suas necessidades de comunicação à administração, fornecendo feedback e orientação.

Externas

Uma comunicação apropriada é necessária, não somente dentro da organização, como também fora dela. Por meio de canais de comunicação abertos, clientes e fornecedores podem fornecer informações altamente significativas referentes ao design ou à qualidade dos produtos ou serviços, possibilitando, assim, a abordagem da organização em relação à evolução das exigências ou preferências do cliente.

Por exemplo, reclamações ou indagações de clientes ou fornecedores relacionadas a embarques, recebimentos, faturamento ou outras atividades, geralmente, indicam a existência de problemas operacionais e, possivelmente, práticas fraudulentas ou outras indevidas. A administração deverá estar sempre pronta para reconhecer as implicações dessas circunstâncias, investigar e adotar as medidas corretivas necessárias, tendo em mente o impacto destas sobre os relatórios financeiros, de conformidade e objetivos operacionais.

É importante haver uma comunicação aberta sobre o apetite a riscos e as tolerâncias a risco da organização, especialmente para as organizações associadas a outras em cadeias de suprimento ou empreendimentos de comércio eletrônico. Nesses casos, a administração leva em conta o modo pelo qual o seu apetite a riscos e a tolerância a riscos estão alinhados com o dos parceiros comerciais, assegurando que a organização não aceitará, por falta de controle, um excesso de riscos de seus parceiros.

A comunicação com partes interessadas, agentes reguladores, analistas financeiros e outras partes externas, disponibiliza informações pertinentes às respectivas necessidades, de maneira que possam entender prontamente as circunstâncias e os riscos que a organização enfrenta. Essa comunicação deve ser significativa, pertinente e oportuna, além de atender às exigências legais e regulatórias.

O comprometimento da administração em estabelecer e manter canais de comunicações com partes externas – independentemente de ser ou não aberta, disponível e rigorosa quanto ao seu acompanhamento – também envia uma mensagem para toda a organização.

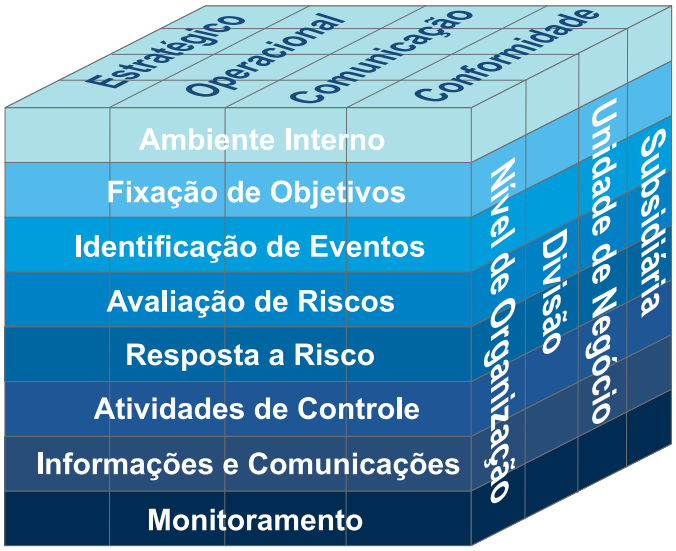
Meios de Comunicação

A comunicação pode surgir sob a forma de manuais de políticas, memorandos, mensagens de correio eletrônico, notificações em quadros de avisos, mensagens pela Internet e mensagens gravadas em vídeo. Se as mensagens são transmitidas verbalmente – em grandes grupos, pequenas reuniões ou sessões individuais – o tom de voz e a linguagem corporal enfatizam aquilo que está sendo transmitido.

A forma pela qual a administração trata o seu pessoal pode transmitir uma mensagem poderosa. Cabe aos gestores lembrar que os atos dizem mais do que as palavras. Seus atos, por sua vez, são influenciados pelo histórico e pela cultura da organização, baseando-se em observações anteriores de como os seus mentores enfrentaram situações semelhantes.

Uma organização com um histórico de integridade nas operações e uma cultura bem entendida pelas pessoas não encontrará muita dificuldade em passar a sua mensagem. Outra sem tradição terá de pôr mais energia na forma em que as mensagens são comunicadas.

9. Monitoramento



Resumo do capítulo: o gerenciamento de riscos corporativos é monitorado, avaliando-se a presença e o funcionamento de seus componentes ao longo do tempo. Essa tarefa é realizada mediante atividades contínuas de monitoramento, avaliações independentes ou uma combinação de ambas. O monitoramento contínuo ocorre no decurso normal das atividades de administração. O alcance e a freqüência das avaliações independentes dependerá basicamente de uma avaliação dos riscos e da eficácia dos procedimentos contínuos de monitoramento. As deficiências no gerenciamento de riscos corporativos são relatadas aos superiores, sendo as questões mais graves relatadas ao Conselho de administração e à diretoria executiva.

O gerenciamento de riscos corporativos de uma organização modifica-se com o passar do tempo. As respostas a risco que se mostravam eficazes anteriormente podem tornar-se inócuas; as atividades de controle podem perder a eficácia ou deixar de ser executadas; ou os objetivos podem mudar. Essas modificações podem ser causadas pela chegada de novos profissionais, pelas mudanças na estrutura ou no direcionamento da organização ou, ainda, pela introdução de novos processos. Diante dessas mudanças, a administração necessita determinar se o funcionamento do gerenciamento de riscos corporativos permanece eficaz.

O monitoramento pode ser conduzido de duas maneiras: mediante atividades contínuas ou de avaliações independentes. Geralmente, os mecanismos de administração de riscos corporativos são estruturados para fazer o próprio monitoramento de forma contínua, no mínimo até um certo ponto. Quanto maior o alcance e a eficácia do monitoramento contínuo, menor a necessidade de avaliações independentes. Fica a critério da administração definir a freqüência necessária de avaliações independentes, de forma a ter garantia razoável da eficácia do gerenciamento de riscos corporativos. Ao fazer essa determinação, a administração leva em conta a natureza e a extensão das mudanças que estão ocorrendo, os riscos associados, a competência e a experiência do pessoal que implementa as respostas a risco e os controles pertinentes, além dos resultados do monitoramento contínuo. Via de regra, uma combinação de monitoramento

contínuo e avaliações independentes será capaz de assegurar que o gerenciamento de riscos corporativos mantenha a sua eficácia com o passar do tempo.

O monitoramento contínuo é incorporado às atividades normais e repetitivas de uma organização. Ele também é conduzido em tempo real, responde dinamicamente a mudanças nas condições e está firmemente arraigado na organização. Conseqüentemente, ele é mais eficaz do que as avaliações independentes. Visto que as avaliações independentes geralmente ocorrem após a constatação de algum fato, os problemas serão identificados com maior rapidez por atividades contínuas de monitoramento. Ainda assim, muitas organizações que possuem sistemas complexos de atividades de monitoramento contínuo realizam periodicamente avaliações independentes do seu gerenciamento de riscos corporativos. A organização que constata a necessidade de conduzir avaliações independentes freqüentemente deverá concentrar-se em fortalecer as suas atividades de monitoramento contínuo.

Atividades de Monitoramento Contínuo

Muitas atividades prestam-se ao monitoramento da eficácia do gerenciamento de riscos corporativos no decurso normal da administração dos negócios. As referidas atividades originam-se das atividades de gestão que podem incluir análises de variância, comparações das informações oriundas de fontes discrepantes e abordagem a ocorrências imprevistas.

Em geral, as atividades de monitoramento contínuo são conduzidas pelos gerentes de operação de linha ou de suporte funcional, que dedicam profunda consideração às implicações das informações que recebem. Ao concentrar-se nos relacionamentos, nas inconsistências ou em outras implicações relevantes, levantam questões, acompanhando outro pessoal, se necessário, para determinar se existe necessidade de adotar medidas corretivas ou outras. As atividades de monitoramento contínuo são diferenciadas das atividades realizadas para o cumprimento da política nos processos do negócio. Por exemplo, as aprovações de transações, as reconciliações de saldos de contas e a verificação da exatidão das mudanças feitas nos arquivos mestres, executadas como etapas necessárias em sistemas de informação ou os processos de contabilidade são mais bem definidas como atividades de controle.

O Anexo 9.1 apresenta exemplos de atividades de monitoramento contínuo.

Anexo 9.1

- Os gerentes que analisam relatórios operacionais, que costumavam administrar operações de forma contínua, podem identificar imprecisões ou exceções em resultados esperados. Por exemplo, os gerentes de vendas, compras e produção nos níveis de divisão, subsidiária e corporativo, e que mantêm contato com as operações, são capazes de questionar os relatórios que apresentem divergências significativas em relação a seu conhecimento das operações. Um relato oportuno e completo e a resolução das referidas exceções fortalecem a eficácia do processo.

- Mudanças nas informações obtidas mediante modelos de valor em risco, utilizados para avaliar os efeitos dos movimentos em potenciais de mercado sobre a posição financeira de uma Companhia, estão relacionadas com as transações financeiras relatadas, considerando os efeitos esperados.

- As comunicações de partes externas comprovam as informações geradas internamente ou indicam a existência de problemas. Por exemplo, o cliente corrobora implicitamente os dados de faturamento ao pagar suas duplicatas. Por outro lado, reclamações de clientes referentes ao faturamento podem indicar deficiências no processamento das transações de venda. Da mesma forma, os relatórios de gestores de investimentos em relação a ganhos, perdas e rendimentos com valores mobiliários, podem comprovar ou apontar problemas com os registros da Companhia (ou do gestor). A revisão das políticas e práticas de segurança de uma seguradora fornece informações sobre a segurança operacional e o desempenho no cumprimento de normas.

- Os agentes normativos comunicam-se com a administração com relação a conformidade ou outras questões que se refletem no funcionamento do gerenciamento de riscos corporativos.

- Auditores externos e internos e assessores fornecem informações periódicas, visando ao fortalecimento do gerenciamento de riscos corporativos. Os auditores podem dedicar atenção considerável a riscos fundamentais e respectivas respostas, bem como ao desenho das atividades de controle. Fraquezas em potencial são identificadas e as respectivas medidas alternativas são recomendadas à administração, acompanhadas de informações úteis na realização de determinações de custo-benefício. Auditores internos ou pessoas que desempenham funções de revisão semelhantes podem ser particularmente eficazes no monitoramento das atividades de uma organização.

- Seminários de treinamento, sessões de planejamento e outras reuniões fornecem à administração importante *feedback* que lhe permite determinar se o gerenciamento de riscos corporativos permanece eficaz. Além dos problemas específicos que podem indicar condições de risco, a consciência de risco e de controle dos participantes geralmente é uma condição aparente.

- O gerente, no decurso normal da administração dos negócios, discute com o seu pessoal a respeito de questões como o entendimento que o referido pessoal tem do código de conduta da organização, de maneira em que os riscos são identificados e as questões que surgem em relação à operação das atividades de controle. Essas discussões servem para confirmar o funcionamento adequado dos elementos do gerenciamento de riscos corporativos ou assuntos emergentes que necessitam de atenção.

Avaliações Independentes

Embora os procedimentos de monitoramento contínuo geralmente forneçam importante feedback sobre a eficácia de outros componentes do gerenciamento de riscos corporativos, pode ser de valia abordar a questão como se fosse a primeira vez, com o enfoque voltado diretamente à eficácia do gerenciamento de riscos corporativos. Esse procedimento também oferece a oportunidade de considerar a eficácia dos procedimentos de monitoramento contínua.

Escopo e Freqüência

As avaliações do gerenciamento de riscos corporativos podem variar em termos de escopo e freqüência, dependendo da significância dos riscos e da importância das respostas a risco e dos respectivos controles para a administração dos riscos. As áreas de riscos e as respostas a risco de alta prioridade tendem a ser avaliadas com mais freqüência. A avaliação da totalidade do gerenciamento de riscos corporativos – que, geralmente, necessita ser realizada com menor freqüência do que a avaliação de partes específicas – pode ser ocasionada por diversos motivos: mudança importante na estratégia ou na administração, aquisições ou distribuições de recursos, mudanças nas condições econômicas ou políticas ou, ainda, mudanças nas operações ou métodos de processamento de informações. Ao se tomar a decisão de empreender uma avaliação detalhada do gerenciamento de riscos de uma organização, deve-se dedicar atenção especial à abordagem de sua aplicação na definição da estratégia e em relação a atividades significativas. O alcance da avaliação também dependerá das categorias de objetivos – estratégicos, operacionais, comunicação e conformidade – que devem ser abordadas.

Quem Conduz a Avaliação

Freqüentemente, as avaliações têm a forma de auto-avaliações nas quais as pessoas responsáveis por uma determinada unidade ou função determinam a eficácia do gerenciamento de riscos corporativos em relação às suas atividades. Por exemplo, o executivo principal de uma divisão dirige a avaliação de suas atividades de administração de riscos corporativos. Esses responsáveis avaliam pessoalmente as atividades de administração de riscos associadas às opções estratégicas e aos objetivos de alto nível, além do componente de ambiente interno, e os indivíduos responsáveis pelas várias atividades operacionais da divisão avaliam a eficácia dos componentes da administração de riscos corporativos em relação às suas esferas de responsabilidade. Os gestores de linhas de negócio enfocam a operação e o cumprimento dos objetivos, e o *controller* da divisão concentra-se nos objetivos de comunicação. As avaliações da divisão são então consideradas pela alta administração com as avaliações de outras divisões da Companhia.

Os auditores internos geralmente avaliam como parte de seus deveres normais, ou mediante solicitação específica do conselho de administração, comitê de auditoria, diretoria ou executivos de subsidiárias ou divisões. Do mesmo modo, a administração poderá utilizar informações dos auditores externos ao considerar a eficácia do gerenciamento de riscos corporativos. Pode-se utilizar uma combinação de esforços na realização de procedimentos de avaliação que a administração julgue necessários.

Processo de Avaliação

A avaliação da administração de riscos corporativos é um processo. Embora as abordagens ou as técnicas possam variar, o processo deverá conter uma disciplina com determinados conceitos básicos.

O avaliador deverá entender cada uma das atividades da organização e cada um dos componentes do gerenciamento de riscos corporativos que está sendo abordado. Pode ser útil concentrar-se primeiramente no funcionamento expresso do gerenciamento de riscos corporativos – às vezes chamada de desenho de sistema ou processo.

O avaliador deve determinar o modo em que o sistema funciona. Os procedimentos destinados a operar de uma certa forma podem ser modificados com o tempo para operar de modo diferente ou podem não ser mais executados. Às vezes, novos procedimentos são estabelecidos, mas não são conhecidos por aqueles que descreveram o processo e não estão incluídos na documentação existente. A determinação do funcionamento real pode ser realizada mediante discussões com o pessoal que executa, ou é afetado pelo gerenciamento de riscos corporativos, mediante exame de registros sobre desempenho ou, ainda, uma combinação de procedimentos.

O avaliador analisa o traçado do processo de administração de riscos corporativos e os resultados dos testes realizados. A análise é realizada novamente em comparação a padrões estabelecidos pela administração para cada um dos componentes, com a meta final de determinar se o processo oferece uma garantia razoável em relação aos objetivos enunciados.

Metodologia

Existe uma variedade de metodologias e ferramentas, inclusive listas de verificação, questionários e técnicas de fluxogramas. Como parte de sua metodologia de avaliação, algumas organizações comparam ou desenvolvem um processo de comparação de indicadores de desempenho para o seu processo de administração de riscos corporativos em relação aos de outras organizações. Uma Companhia poderá, por exemplo, comparar o seu gerenciamento de riscos corporativos em relação às Companhias que desfrutam de renome nessa área. As comparações podem ser feitas diretamente ou sob os auspícios de associações de classe ou da indústria. Outras organizações podem fornecer informações comparativas, e as funções equivalentes de revisão permitindo que algumas indústrias avaliem o seu gerenciamento de riscos corporativos diante de seus pares. Porém, certa cautela é necessária ao estabelecer comparações, devendo ser considerada diferenças existentes nos objetivos, nos fatos e nas circunstâncias. Além disso, todos os oito componentes do gerenciamento de riscos corporativos devem ser considerados, bem como as limitações inerentes a cada organização.

Documentação

A quantidade de documentação do gerenciamento de riscos corporativos de uma organização varia de acordo com o tamanho, a complexidade e os fatores semelhantes. As grandes organizações geralmente possuem documentação escrita, como manuais de política, organogramas formais, descrições de cargo, instruções de operação, fluxogramas de sistemas e assim por diante. As organizações menores possuem uma documentação consideravelmente menor. Muitos aspectos do gerenciamento de riscos corporativos são informais e não estão documentados, apesar disso são executados com regularidade e altamente

eficazes. Essas atividades podem ser testadas da mesma forma que as atividades documentadas. O fato dos elementos do gerenciamento de riscos corporativos não estarem documentados não significa que não sejam eficazes ou não possam ser avaliados. Contudo, um nível apropriado de documentação geralmente implica maior eficácia e eficiência às avaliações.

O avaliador poderá decidir documentar o próprio processo de avaliação. Ele basear-se-á na documentação existente do gerenciamento de riscos corporativos da organização. Tipicamente, o processo será suplementado por documentação adicional, com descrições dos testes e das análises conduzidas na avaliação.

Se a administração julgar conveniente fazer uma declaração às partes externas em relação à eficácia do gerenciamento de riscos corporativos, esta deverá considerar se desenvolve e retém a documentação de suporte às suas declarações. Essa documentação poderá ser útil, caso a declaração seja questionada.

Relato de Deficiências

As deficiências no gerenciamento de riscos corporativos de uma organização podem ter diversas origens, inclusive os procedimentos de monitoramento contínuo, avaliações independentes e partes externas. Uma deficiência é uma condição do gerenciamento de riscos de uma organização que merece atenção e que pode representar uma desvantagem real, percebida ou em potencial, ou uma oportunidade de fortalecer o gerenciamento de riscos corporativos para aumentar a probabilidade dos objetivos serem alcançados.

Fontes de Informações

Uma das melhores fontes de informação sobre deficiências no gerenciamento de riscos corporativos é o próprio processo de gestão. As atividades de monitoramento contínuo de uma organização, inclusive as atividades gerenciais e a supervisão diária dos empregados, proporcionam idéias com base nas pessoas que estão diretamente envolvidas nas atividades. Esses *insights* são adquiridos em tempo real e podem possibilitar uma rápida identificação das deficiências. Outras fontes de deficiências são as avaliações independentes do processo de gerenciamento de riscos. As avaliações realizadas pela administração, pelos auditores internos ou por outras funções podem identificar áreas com necessidade de melhoria.

Freqüentemente, as partes externas fornecem informações importantes sobre a atuação do gerenciamento de riscos corporativos de uma organização. Essas partes podem ser clientes, revendedores e outras pessoas que realizam transações com a organização, auditores externos e agentes reguladores. Os relatórios de fontes externas devem ser cuidadosamente considerados em decorrência de suas implicações para o gerenciamento de riscos corporativos, devendo, assim, adotar em seguida as medidas corretivas adequadas.

O Que é Comunicado

O que deve ser relatado? Embora não exista uma resposta universal, certos parâmetros podem ser estabelecidos.

Todas as deficiências de administração de riscos corporativos identificadas, capazes de afetar a capacidade da organização de desenvolver e implementar a sua estratégia, bem como de fixar e alcançar os seus objetivos, devem ser relatadas para que sejam adotadas as medidas necessárias. A natureza das questões a serem comunicadas variará dependendo da autoridade que as pessoas têm de tratar das circunstâncias que surgem e sob a supervisão de seus superiores. Ao se considerar o que deve ser comunicado, é necessário observar as implicações das falhas constatadas. É essencial que não apenas uma determinada transação ou evento seja comunicado, como também os procedimentos potencialmente falhos envolvidos e passíveis de reavaliação.

Pode-se argumentar que nenhum problema é tão significativo a ponto de justificar uma investigação de suas implicações. Um empregado que furta alguns dólares de um caixa para uso pessoal, por exemplo, não seria significativo em termos desse evento específico, e também não o seria em termos de todo o valor transitado no caixa. Desse modo, não valeria a pena realizar uma investigação. Entretanto, essa aparente tolerância em relação ao uso pessoal do dinheiro da organização pode enviar mensagens indesejáveis ao restante dos funcionários.

Além das deficiências, as oportunidades identificadas para aumentar a probabilidade dos objetivos da organização serem alcançados também devem ser comunicadas.

A Quem Comunicar

As informações geradas no decorrer das atividades operacionais são geralmente comunicadas pelos canais normais aos superiores imediatos. Estes, por sua vez, podem estender a comunicação em direção ascendente ou lateral na organização, de modo que as informações acabem nas mãos de pessoas que podem e devem atuar em relação a estas. Canais de comunicação alternativos também devem existir para o relato de informações sensíveis, como atos ilegais ou impróprios. As constatações de deficiências no gerenciamento de riscos corporativos comumente devem ser relatadas não apenas à pessoa responsável pela função ou atividade em questão, como também pelo menos a um nível de chefia acima dessa pessoa. Esse nível de chefia superior fornece o necessário suporte ou supervisão para a adoção de medidas corretivas e ele é orientado a comunicar-se com outras pessoas na organização, cujas atividades podem ser afetadas. Caso o efeito da constatação estenda-se além dos limites da organização, o relatório deverá também fazer o mesmo e ser dirigido a um nível suficientemente elevado para assegurar que medidas apropriadas serão tomadas.

Diretivas de Informação

O fornecimento das informações necessárias à parte cabível, dêem relação às deficiências no gerenciamento de riscos corporativos, é um fator crítico. Os protocolos devem ser estabelecidos para identificar quais informações são necessárias em um dado nível para um processo decisório eficaz.

Esses protocolos refletem na regra geral de que um gestor deve receber as informações que afetam os atos ou o comportamento do pessoal sob a sua responsabilidade, bem como as informações necessárias para a realização de determinados objetivos. Normalmente, um presidente gostaria de ser notificado, por exemplo, com relação a graves infrações às políticas ou aos procedimentos. Essa pessoa também desejaria obter informações de apoio sobre questões que possam trazer um impacto significativo ou implicações estratégicas ou, até mesmo, que possam afetar a reputação da organização.

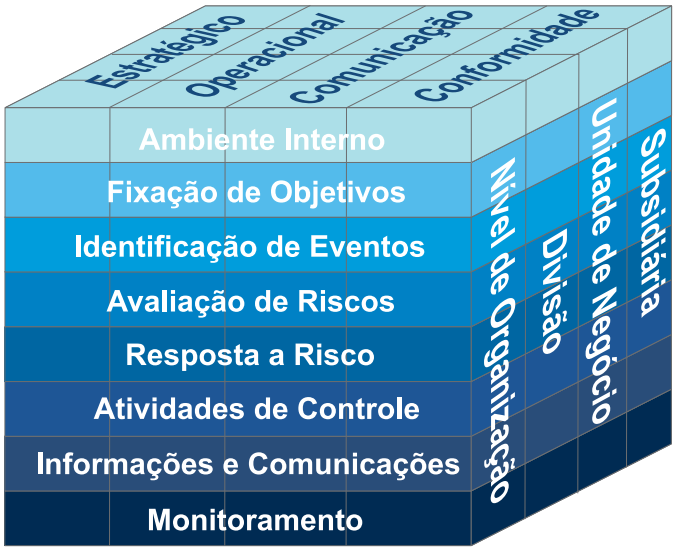
Um executivo sênior deve ser notificado em relação ao gerenciamento de riscos e controlar as deficiências capazes de afetar a sua unidade. Os exemplos incluem circunstâncias, nas quais bens de um valor monetário específico não estão adequadamente protegidos, falta de competência dos empregados, ou quando reconciliações financeiras importantes não são executadas adequadamente. Os gestores devem ser informados das deficiências em suas unidades em níveis cada vez mais detalhados à medida que descemos ao longo da estrutura da organização.

Os supervisores definem os protocolos de comunicação para os subordinados. O grau de especificidade poderá variar, geralmente aumentando nos níveis inferiores da organização. Enquanto os protocolos de relatórios possam inibir a eficácia, caso sejam definidos com rigor excessivo, poderão otimizar a comunicação, se houver flexibilidade suficiente.

As partes para as quais as deficiências devem ser comunicadas, às vezes fornecem instruções específicas em relação à aquilo que deve ser relatado. O Conselho de administração, a diretoria executiva ou comitê de auditoria, por exemplo, poderá solicitar à administração ou aos auditores internos ou externos que comuniquem apenas as deficiências que atingirem um parâmetro específico de gravidade ou importância.

10. Funções e Responsabilidades

Resumo do capítulo: todos os membros de uma organização possuem alguma responsabilidade pelo gerenciamento de riscos corporativos. O presidente é o responsável principal e deve assumir a sua “titularidade”. Outros gerentes apóiam a filosofia de administração de riscos, promovem o cumprimento do apetite a riscos e administram os riscos dentro de suas esferas de responsabilidade e adequada as tolerâncias a riscos. As demais pessoas são responsáveis pelo gerenciamento de riscos corporativos, segundo políticas e protocolos estabelecidos. A diretoria executiva fornece uma importante supervisão à administração de riscos corporativos. Inúmeras partes externas geralmente fornecem informações úteis para a condução do gerenciamento de riscos corporativos, porém não respondem pela sua eficácia.



O gerenciamento de riscos corporativos é realizado por inúmeros agentes, cada uma deles com importantes responsabilidades. A diretoria executiva (diretamente ou por meio de seus comitês), a administração, os auditores internos e as outras equipes internas prestam contribuições importantes à administração de riscos. Outros agentes como auditores externos e órgãos reguladores, muitas vezes, estão diretamente associados às avaliações de risco e aos controles internos. Entretanto existe uma diferença entre os que fazem parte do processo de administração dos riscos corporativos, e os que não fazem parte, porém cujas ações podem afetar o processo ou ajudar a organização a alcançar os seus objetivos. O fato de um agente externo contribuir direta ou indiretamente para que uma organização alcance os seus objetivos não o torna parte, nem responsável pelo gerenciamento de riscos corporativos da organização.

Pessoal da Organização

A diretoria executiva, a administração, os executivos de riscos, os executivos de finanças, os auditores internos e, na verdade, qualquer indivíduo dentro de uma organização pode contribuir para a gestão mais eficaz dos riscos corporativos.

Conselho de Administração

A administração reporta à diretoria executiva ou ao conselho de administração, o qual fornece supervisão, liderança e direcionamento. Ao escolher a diretoria executiva, o conselho de administração tem uma importante função ao definir aquilo que espera em termos de integridade, valores éticos e, mediante suas atividades de supervisão, poderá determinar se as expectativas estão sendo ou não atendidas. Da mesma forma, ao reservar sua autoridade a certas decisões fundamentais, o conselho de administração desempenha uma função de fixação de estratégias, formulação de objetivos de alto nível e alocação de recursos de modo mais amplo.

O conselho de administração supervisiona o gerenciamento de riscos corporativos da organização ao:

- saber até que ponto a administração estabeleceu um gerenciamento de riscos corporativos eficaz;
- estar ciente e de acordo com o apetite a riscos;
- revisar a visão de portfólio dos riscos assumidos em contraste com o apetite a riscos;
- ser notificada em relação aos riscos mais significativos e saber se a administração está respondendo adequadamente.

O conselho de administração faz parte do componente ambiente interno e deve ter a composição e o enfoque necessários para que o gerenciamento de riscos corporativos possa ser eficaz.

Os membros do conselho de administração efetivos devem ser objetivos, capazes e inquisitivos. Devem possuir um conhecimento prático das atividades da organização e de seu ambiente, bem como dedicar o tempo necessário para cumprir suas responsabilidades de conselheiro. Despendem recursos quando necessário para realizar investigações especiais e ter uma comunicação aberta e irrestrita com os auditores internos e externos, bem como com os assessores jurídicos.

O conselho de administração poderá utilizar comitês para cumprir determinadas obrigações. A utilização e o enfoque dos comitês podem variar de uma organização para outra, embora os mais comuns sejam de nomeação/governança corporativa, remuneração e auditoria, cada qual com o seu enfoque nos elementos de administração de riscos da organização. O comitê de nomeação, por exemplo, identifica e analisa as qualificações de possíveis membros do conselho; o comitê de remuneração analisa a adequação dos sistemas de recompensa, equilibrando programas motivacionais saudáveis com a necessidade de evitar desnecessárias tentações de manipular os indicadores adotados na definição da remuneração. O comitê de auditoria tem a responsabilidade direta sobre a confiabilidade das comunicações externas e deve reconhecer os riscos relativos a uma comunicação confiável dos relatórios financeiros. Assim sendo, o conselho de administração e os seus comitês fazem parte importante do gerenciamento de riscos corporativos.

A Diretoria executiva

A diretoria executiva é diretamente responsável por todas as atividades de uma organização, inclusive do gerenciamento de riscos corporativos. Naturalmente, os diretores em seus diferentes níveis terão diferentes responsabilidades no gerenciamento de riscos corporativos. Essas responsabilidades podem variar consideravelmente, dependendo das características da organização.

Em qualquer organização, o presidente é o depositário final da responsabilidade de gestão de riscos. Um dos aspectos mais importantes dessa responsabilidade é assegurar a presença de um ambiente interno positivo. Mais do que qualquer outro indivíduo ou função, o presidente estabelece o tom na cúpula que influencia os fatores ambientais internos e outros componentes do gerenciamento de riscos corporativos. O presidente também pode ter influência sobre o conselho de administração ao direcionar a identificação de novos membros para o próprio conselho, dando o exemplo para atrair ou repelir os possíveis candidatos. Com freqüência cada vez maior, os candidatos ao conselho observam atentamente a integridade e os valores da diretoria executiva para determinar se aceitam ou não uma indicação. Os diretores em potencial também concentram-se no gerenciamento de riscos corporativos da organização para verificar se esta possui o embasamento crítico de integridade e valores éticos para permitir a sua eficácia.

As responsabilidades do presidente incluem certificar-se que todos os componentes do gerenciamento de riscos corporativos estejam implementados. O presidente geralmente cumpre com as suas atribuições:

- Fornecendo liderança e direcionamento à diretoria executiva. Em conjunto com eles, o presidente forma os valores, os princípios e as principais políticas operacionais que constituem o alicerce da gestão de riscos corporativos na organização. O presidente e a diretoria executiva definem os objetivos estratégicos, a estratégia e os objetivos associados de alto nível. E, estabelecem também, políticas de caráter mais amplo e desenvolvem a filosofia de gestão de riscos, apetite a riscos e a cultura da organização. Adotam medidas em relação à estrutura organizacional, ao conteúdo e à comunicação de políticas fundamentais da organização, bem como do tipo de sistemas de planejamento e de comunicação que será utilizada.
- Reunindo-se periodicamente com os diretores responsáveis pelas principais áreas funcionais – vendas, marketing, produção, obtenção, finanças, recursos humanos – para revisar suas responsabilidades, inclusive a forma em que administram riscos. O presidente adquire conhecimento dos riscos inerentes às operações, às respostas a riscos e às melhorias de controle necessárias, bem como à condição das iniciativas em andamento. Para desincumbir-se dessas responsabilidades, o presidente deverá definir claramente as informações de que necessita.

Com esses conhecimentos, o presidente estará em condições de monitorar as atividades e os riscos em relação ao apetite a riscos da organização. No caso de alteração das circunstâncias, surgimento de riscos, implementação de estratégias ou ações antecipadas indicam desalinhamento potencial em relação ao apetite a riscos da organização, o presidente adotará as medidas necessárias para restabelecer o alinhamento, ou, ainda, discutir com o conselho de administração as medidas a serem adotadas, ou ainda, se o apetite a riscos da organização deve ser ajustado.

Os diretores encarregados das unidades organizacionais são responsáveis pela administração dos riscos relativos aos objetivos de suas unidades. Essas pessoas transformam estratégias em operações, identificam eventos, avaliam riscos e adotam respostas a riscos. Além

disso, orientam a aplicação dos componentes do gerenciamento de riscos corporativos em suas esferas de responsabilidade, certificando-se de que a sua aplicação esteja consistente com as tolerâncias a riscos. Nesse sentido, a responsabilidade flui em cascata, na qual cada executivo torna-se efetivamente um presidente de sua esfera de responsabilidade.

A diretoria executiva geralmente atribui a responsabilidade pelos procedimentos específicos de gestão de riscos corporativos aos gerentes de processos, funções ou departamentos. Dessa maneira, esses gerentes desempenham um papel mais prático no planejamento e na execução de determinados procedimentos de gestão de riscos relacionados aos objetivos da unidade, como técnicas para a identificação de eventos e avaliação de riscos, bem como na determinação de respostas aos riscos, como o desenvolvimento de protocolos para a compra de matérias-primas ou a aprovação de novos clientes. Eles também fazem recomendações referentes a atividades de controle relacionadas, monitoram sua aplicação e reúnem-se com os diretores para relatar o funcionamento das atividades de controle.

Os procedimentos acima envolvem o levantamento de eventos ou as condições externas, os erros na entrada de dados, ou nas transações que aparecem nos relatórios de exceção, analisando os motivos das variações no orçamento das despesas departamentais e acompanhando, desses modo, os pedidos pendentes ou as posições de estoque de produtos. As questões significativas, sejam elas relativas a uma determinada transação ou indicação de uma maior preocupação, devem ser comunicadas aos superiores na organização.

As funções de suporte, como recursos humanos, conformidade ou jurídico, também apresentam importantes funções de apoio no desenho ou na constituição de componentes eficazes de gestão de riscos corporativos. Os recursos humanos poderão formular e ajudar a implementar programas de treinamento no código de conduta da organização e em outras questões políticas mais amplas, geralmente introduzidas com a liderança da unidade de negócios. A função jurídica disponibiliza informações aos gerentes de linha de negócio relacionados a novas leis e regulamentos que afetam as políticas operacionais, e/ou junto com os executivos de compliance fornecem informações críticas se as transações ou os protocolos planejados estão em conformidade com requisitos legais e éticos.

As responsabilidades dos diretores devem contemplar autoridade e responsabilidade por ações tomadas (prestação de contas). Cada diretor será cobrado pelo nível hierárquico imediatamente superior, quanto a parte do gerenciamento de riscos corporativos que lhe cabe, ficando com o presidente a responsabilidade final perante o conselho de administração. Embora diferentes níveis hierárquicos possuam diferentes responsabilidades e funções na gestão de riscos, as suas ações deverão compor-se na gestão de riscos corporativos de toda a organização.

Responsável pela Gestão de Riscos

Algumas organizações adotam coordenação centralizada para facilitar o gerenciamento de riscos corporativos. O responsável pela gestão de riscos – em algumas organizações denominado executivo chefe de riscos ou gerente de riscos – trabalha com outros gerentes para estabelecer um processo de gestão de riscos eficaz em suas áreas de responsabilidade. Tendo sido nomeado pelo presidente e sob os seus auspícios diretos, o funcionário responsável por riscos possui os recursos com o intuito de ajudar a gestão efetiva dos riscos corporativos nas subsidiárias, unidades de negócios, departamentos, funções e atividades. O profissional responsável por riscos tem a incumbência de monitorar o progresso e ajudar os demais gerentes a comunicar as

informações relevantes sobre riscos a seus superiores, subordinados e pares na organização. O empregado responsável por riscos também poderá servir de canal de comunicação complementar.

Algumas organizações atribuem essa função a outro funcionário graduado, como o diretor executivo financeiro, assessor jurídico, diretor de auditoria interna ou de compliance; outras organizações constataram que a magnitude e o alcance dessa função requerem atribuição e recursos independentes.

Companhias constataram que essa função é muito bem-sucedida quando estabelecida, claramente, sua responsabilidade com função de suporte – apoiando e facilitando as gerências de linha de negócio. Para que o gerenciamento de riscos corporativos tenha eficácia, os gerentes de linha devem assumir responsabilidade primária e responder pelo gerenciamento de riscos em suas respectivas áreas.

Entre as responsabilidades de um funcionário responsável por riscos estão:

- estabelecer as políticas de administração de riscos, inclusive definir funções e responsabilidades, e participar da fixação de metas para implementação;
- constituir autoridade e responsabilidade pelo gerenciamento de riscos corporativos nas unidades de negócios;
- promover a competência em gerenciamento de riscos corporativos pela Companhia, bem como facilitar o desenvolvimento de conhecimentos especializados técnicos de gestão de riscos e ajudar os gerentes a alinhar as respostas com as tolerâncias a risco, além de desenvolver os controles adequados;
- orientar a integração do gerenciamento de riscos corporativos com outras atividades de planejamento e administração de negócios;
- estabelecer uma linguagem comum de gestão de riscos que inclua medidas comuns para probabilidade, impacto e categorias de riscos;
- facilitar o desenvolvimento de protocolos de comunicação pela administração, inclusive limites quantitativos e qualitativos, bem como monitoramento do processo de comunicação;
- comunicar ao presidente o andamento, as situações excepcionais e as recomendação de ações, quando necessário.

Executivos Financeiros

Os executivos de finanças e de controle e suas equipes possuem significado particularmente importante nas atividades de gerenciamento de riscos corporativos, pois suas ações atingem de forma ascendente e descendente todas as unidades operacionais e de negócios. Esses executivos financeiros geralmente envolvem-se no desenvolvimento de planos e orçamentos para toda a organização, além de realizar o acompanhamento e a análise de desempenho, a partir de uma perspectiva da operação, informação e compliance. Freqüentemente, essas atividades fazem parte de uma visão central ou “corporativa,” mas, comumente, também apresenta alçada de aprovação na supervisão das atividades da divisão, subsidiária ou de outras unidades. Desse modo, os executivos financeiro, contábil, *controller* e outros agentes da área financeira são essenciais ao modo como a administração exerce o gerenciamento de riscos corporativos. Esses executivos desempenham um papel importante na prevenção e na identificação de informação fraudulenta, e, na qualidade de membro da alta administração, o executivo financeiro contribui para estabelecer o tom da conduta ética da organização; a implementação e o monitoramento dos sistemas de comunicação tem sobre si importante responsabilidade pelas demonstrações financeiras e influencia seu desenho.

Examinando-se os componentes do gerenciamento de riscos corporativos torna-se evidente que o executivo financeiro e seu pessoal desempenham papéis essenciais. Esse diretor é fundamental no estabelecimento de objetivos, na formulação das estratégias, na análise de riscos e na tomada de decisões sobre como as mudanças capazes de afetar a organização serão administradas. Fornece informações valiosas e direcionamento, sendo posicionada para concentrar-se na supervisão e no acompanhamento das medidas adotadas.

Desse modo, o executivo financeiro deve sentar-se à mesa como um par dos demais diretores. Qualquer tentativa da administração de limitar o seu campo de ação às principais áreas, por exemplo, de informações financeiras e tesouraria, poderá limitar seriamente a capacidade de crescimento da organização.

Auditores Internos

Os auditores internos desempenham uma função essencial ao avaliar a eficácia do gerenciamento de riscos corporativos e ao recomendar melhorias. As normas estabelecidas pelo Institute of Internal Auditors no Brasil: estipulam que o alcance da auditoria interna deve incluir o gerenciamento de riscos e os sistemas de controle. Essa tarefa compreende a avaliação da confiabilidade das informações, a eficácia e a eficiência das operações e o cumprimento de leis e normas aplicáveis. Ao incumbir-se de suas responsabilidades, os auditores internos assistem a administração e o conselho de administração ou o comitê de auditoria no exame, na avaliação, na comunicação e na recomendação de melhorias para uma maior adequação e eficácia do gerenciamento de riscos corporativos da organização.

As normas do *Institute of Internal Auditors* também tratam das funções consideradas apropriadas à auditoria interna, deixando claro que os auditores internos devem ser objetivos em relação às atividades que auditam. Essa objetividade deve refletir em sua posição e sua autoridade dentro da organização e nas atribuições de seu pessoal. A posição e a autoridade organizacional envolvem questões como um canal de comunicação com um indivíduo que possui autoridade suficiente para assegurar cobertura, consideração e resposta adequada de auditoria; acesso ao conselho de administração ou ao comitê de auditoria; e autoridade para o seguimento e o acompanhamento de constatações e recomendações. A seleção e a demissão do executivo-chefe de auditoria somente poderão ser efetuadas com a anuência do conselho de administração ou do comitê de auditoria.

Demais funcionários da Organização

Até certo ponto, o gerenciamento de riscos corporativos é responsabilidade de todos aqueles que trabalham em uma organização, devendo, portanto, fazer parte explícita ou implícita da descrição do cargo. Essa suposição é verdadeira com base em duas perspectivas:

- Praticamente todo o pessoal desempenha alguma função na condução do gerenciamento de riscos. Esse pessoal poderá gerar informações para utilizar na identificação ou avaliação de riscos, ou adoção de outras medidas necessárias à realização do gerenciamento de riscos corporativos. O cuidado com o qual essas atividades são desempenhadas afeta diretamente a eficácia da gestão de riscos na organização.

- Todas as pessoas são responsáveis pelo apoio aos fluxos de informações e comunicações inerentes ao gerenciamento de riscos corporativos. Essa responsabilidade inclui a comunicação a um nível organizacional mais elevado, de quaisquer problemas nas operações, no descumprimento do código de conduta, ou em outras infrações às políticas ou em atos ilegais. A gestão de riscos corporativos depende de controles, inclusive da segregação de funções, e que o pessoal “não faça vista grossa”. Os funcionários necessitam entender que é preciso resistir à pressões dos superiores para participar de atividades ilegítimas, devendo existir outros canais além das linhas regulares de comunicação que possibilitem a denúncia dessas circunstâncias.

O gerenciamento de riscos corporativos é do interesse de todos, devendo as funções e as responsabilidades de todo o pessoal ser nitidamente definidas e comunicadas com eficácia.

Terceiros

Inúmeros terceiros podem contribuir para a realização dos objetivos de uma organização, às vezes mediante ações paralelas às adotadas pela própria organização. Em outros casos, as partes externas podem fornecer informações úteis à organização em suas atividades de gerenciamento de riscos corporativos.

Auditores Externos

Os auditores externos possibilitam à administração e ao conselho de administração uma visão singular, independente e objetiva, que pode contribuir para que a organização realize os seus objetivos de comunicação externa de informações financeiras, bem como outras metas.

Em uma auditoria de demonstrações financeiras, o auditor expressa a sua opinião referente à fidedignidade das demonstrações financeiras em conformidade com princípios contábeis geralmente aceitos, contribuindo, assim, para o cumprimento dos objetivos de comunicação de informações financeiras da organização. O auditor que conduz uma auditoria nas demonstrações financeiras pode contribuir para a realização desses objetivos ao fornecer informações úteis para que a administração cumpra com as suas responsabilidades relativas à gestão de riscos. Essas informações incluem:

- constatações de auditoria, informações analíticas e recomendações das medidas necessárias ao atendimento dos objetivos estabelecidos;
- as constatações de deficiências na administração e os controles de riscos que atraem a atenção do auditor, bem como as recomendações de melhoria.

Freqüentemente, essas informações não estarão apenas relacionadas com as atividades de comunicação, como também a atividades estratégicas, operacionais e de compliance, que poderão trazer importantes contribuições para a realização dos objetivos da organização em cada uma dessas áreas. As informações são relatadas à administração e, dependendo de sua importância, ao conselho de administração ou ao comitê de auditoria.

É importante reconhecer que uma auditoria de demonstrações financeiras, por si só, geralmente não se concentra apenas no gerenciamento de riscos corporativos e, de qualquer modo, não gerará uma opinião do auditor relacionadas à gestão de riscos da organização. Contudo, se for exigido por

lei que o auditor avalie as declarações de uma organização, relacionadas com o controle interno das demonstrações financeiras e as informações em que se fundamentam essas declarações, o alcance do trabalho dirigido a essas áreas será extensivo para que todas as informações adicionais e as evidências possam ser obtidas.

Legisladores e Órgãos Reguladores

Legisladores e órgãos reguladores afetam o gerenciamento de riscos corporativos de muitas organizações mediante requisitos sobre o estabelecimento de mecanismos de gestão de riscos ou controles internos, ou por meio de inspeções por determinadas entidades. Muitas das leis e regulamentos relevantes tratam basicamente dos riscos e controles de informações financeiras. Porém, algumas delas – especialmente aquelas que se aplicam aos órgãos do governo – também podem tratar de objetivos operacionais e de compliance. Muitas organizações estão sujeitas, há muito tempo, a requisitos legais de controle interno. Por exemplo, as Companhias abertas dos Estados Unidos são obrigadas a estabelecer e manter sistemas de controle da contabilidade interna que atendam aos objetivos específicos. A legislação mais recente exige que a diretoria executiva de Companhias abertas (com ações transacionadas em bolsa) certifique a eficácia do controle interno da Companhia sobre os informes financeiros com as declarações de auditores.

Vários órgãos reguladores fiscalizam diretamente as organizações sobre as quais possuem responsabilidades de supervisão. Por exemplo, inspetores de bancos centrais conduzem o exame de bancos e, comumente, concentram-se nos aspectos do gerenciamento de riscos do banco e nos seus sistemas internos de controle. Esses órgãos fazem recomendações e adotam procedimentos para cumprir a lei.

Portanto, os legisladores e os órgãos reguladores afetam o gerenciamento de riscos corporativos de duas formas. Primeiramente, ao estabelecer normas que fornecem o estímulo para que a administração assegure que a gestão de riscos e os sistemas de controle atendam aos requisitos mínimos legais e estatutários. Posteriormente, após as inspeções em uma determinada organização, eles fornecerão informações úteis para a organização sobre a aplicação de gerenciamento de riscos corporativos e as correspondentes recomendações, e, às vezes, as diretrizes para a administração em relação às melhorias necessárias.

Agentes que Interagem com a Organização

Clientes, revendedores, parceiros comerciais e outros que mantêm negócios com uma organização representam importante fonte de informações que podem ser utilizadas nas atividades de gestão dos riscos corporativos. As informações podem ser as mais variadas possíveis, ou seja, informações referentes à demanda emergente para um novo produto ou serviço, discrepâncias de embarque ou faturamento, às questões de qualidade, ou aos atos praticados por empregados que ultrapassam os limites da integridade e da ética. Essas informações podem ser extremamente importantes para que a organização atinja os seus objetivos estratégicos, operacionais, de comunicação e *compliance*. A organização deverá possuir mecanismos implementados para o recebimento dessas informações e a adoção das medidas adequadas. As medidas necessárias não se limitam apenas ao tratamento da situação específica relatada, mas também à investigação da causa subjacente do problema e à sua correção.

Além dos clientes e dos vendedores, outras partes, como credores, podem supervisionar a realização dos objetivos da organização. Um banco, por exemplo, poderá solicitar relatórios de conformidade da contra-parte, como cláusula em determinados

contratos de financiamento. Esse banco também poderá recomendar indicadores de desempenho ou outras metas ou controles desejados.

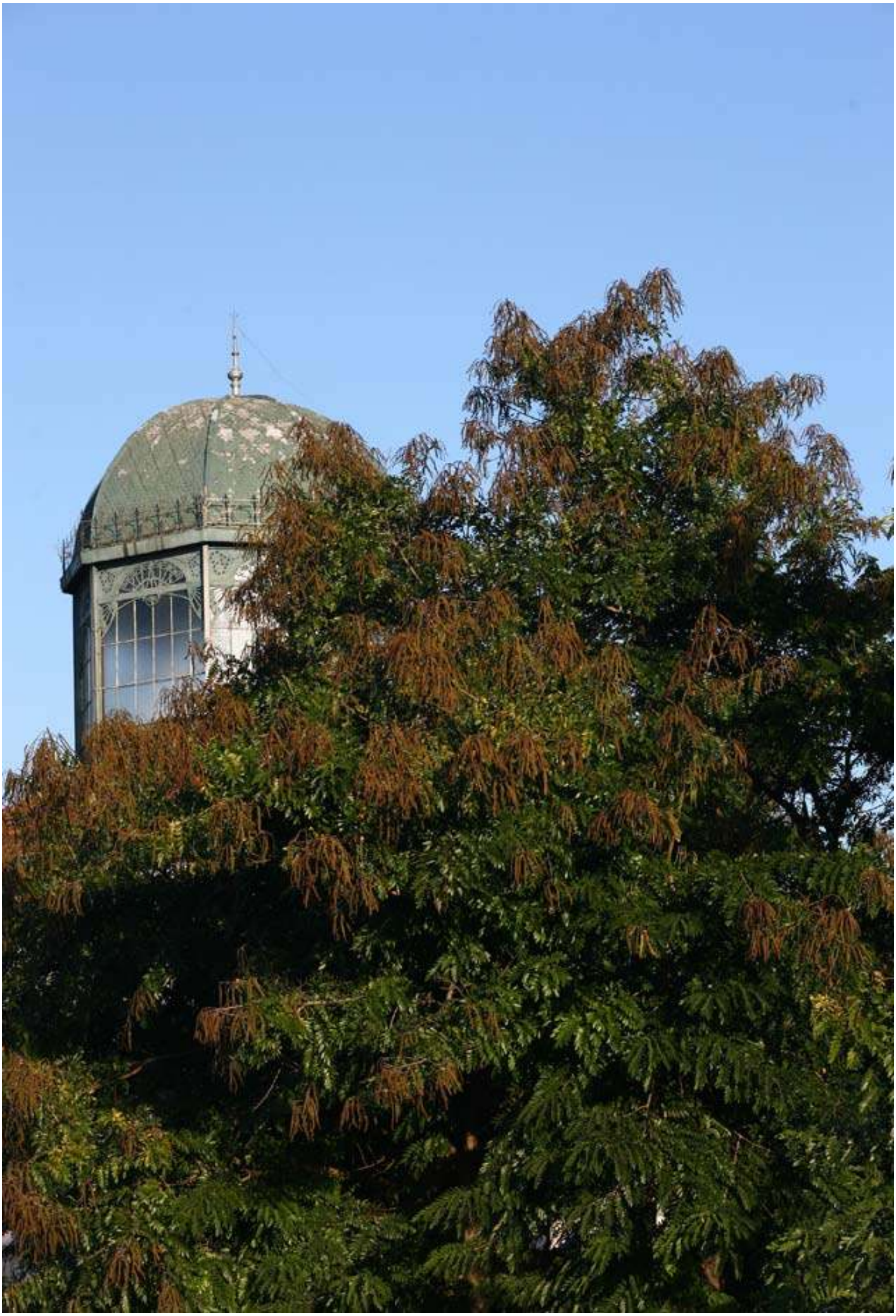
Fornecedores de Serviços Terceirizados

Muitas organizações terceirizam funções comerciais, delegando a sua administração do dia-a-dia a fornecedores externos. Operações administrativas, financeiras e internas são, às vezes, terceirizadas com a finalidade de obter acesso a melhor capacitação e menor custo de serviços. Uma instituição financeira poderá terceirizar o seu processo de revisão de empréstimos; uma empresa de tecnologia poderá terceirizar a operação e a manutenção de seu processamento de dados; e uma Companhia varejista poderá terceirizar a sua função de auditoria interna. Embora esses terceiros executem atividades pela organização e em seu nome, a administração não poderá abdicar da responsabilidade de gerenciar os riscos associados, devendo, dessa forma, implementar um programa para monitorar essas atividades.

Analistas Financeiros, Agências de *Rating*, Mídia Jornalística

Os analistas financeiros e as agências de classificação de risco consideram muitos fatores pertinentes para julgar a oportunidade de investimento em uma organização. Eles analisam a estratégia e os objetivos da administração, as demonstrações financeiras históricas e as informações financeiras prospectivas, as medidas adotadas em resposta às condições da economia e do mercado, o potencial de sucesso a curto e longo prazos, o desempenho da indústria e as comparações seus pares. A mídia impressa e a de difusão, especialmente repórteres financeiros, também podem empreender análises semelhantes.

As atividades de investigação e de monitoramento desses agentes podem fornecer *insights* referentes à forma em que outros percebem o desempenho da organização, a indústria e os riscos econômicos que esta enfrenta, as estratégias inovadoras operacionais ou financeiras que podem melhorar seu desempenho, bem como as tendências da indústria. Essas informações são obtidas em reuniões entre as partes, ou indiretamente mediante análises para os atuais investidores, os em potencial e o público. De qualquer modo, a administração deve considerar as observações e os *insights* de analistas financeiros, as agências de *rating* e a mídia jornalística, que poderão aprimorar o processo de gestão de riscos corporativos.



11. Limitações da Gestão de Riscos Corporativos

Resumo do capítulo: o efetivo gerenciamento de riscos corporativos, não importa o quanto seja bem projetado e operado, apenas proporcionará uma segurança razoável, à administração e ao conselho de administração, quanto ao cumprimento dos objetivos de uma organização. A realização dos objetivos é afetada por limitações inerentes a todos os processos administrativos. Essas limitações incluem o fato que o julgamento humano no processo decisório pode falhar, e que os colapsos podem ocorrer em decorrência dessas falhas humanas, como erros ou equívocos simples. Além disso, os controles podem ser neutralizados por conluio de dois ou mais indivíduos, e a administração dispõe da capacidade de desabilitar o processo de gestão de riscos corporativos, inclusive decisões de resposta a risco e atividades de controle. Outro fator limitante é a necessidade de considerar os custos e os benefícios associados às respostas a riscos.

Para alguns observadores, o gerenciamento de riscos corporativos, como controles internos implantados, assegura que a organização não fracassará – isto é, ela sempre atingirá seus objetivos. Essa opinião é falaciosa.

Considerando as limitações do gerenciamento de riscos corporativos, três conceitos distintos devem ser reconhecidos:

- Primeiro, o risco está relacionado ao futuro, o qual é intrinsecamente incerto.
- Segundo, o gerenciamento de riscos corporativos – mesmo que eficaz – opera em diferentes níveis com relação a diferentes objetivos. No caso de objetivos estratégicos e operacionais, o gerenciamento de riscos corporativos pode contribuir para assegurar que a administração e o conselho de administração em seu papel de supervisão estão oportunamente cientes apenas da evolução da organização no cumprimento desses objetivos. Mas não são capazes de fornecer nem uma garantia razoável de que as próprias metas serão atingidas.
- Terceiro, o gerenciamento de riscos corporativos não é capaz de oferecer uma garantia absoluta em relação a qualquer uma das categorias de objetivos.

A primeira limitação reconhece o fato de que ninguém é capaz de prever o futuro com absoluta certeza. O segundo, reconhece que determinados eventos estão simplesmente além do controle da administração. O terceiro relaciona-se ao fato de que nenhum processo nunca executará exatamente o que foi previsto.

A garantia razoável não implica que o gerenciamento de riscos corporativos fracassará com freqüência. Muitos fatores, isolados ou em conjunto, reforçam o conceito da segurança razoável. O efeito cumulativo das respostas a risco que atendem a diversos objetivos e a natureza de múltiplas finalidades dos controles internos, reduzem o risco de uma organização deixar de atingir os seus objetivos. Além do mais, as atividades operacionais normais do dia-a-dia e as responsabilidades das pessoas que atuam nos diversos níveis de uma organização estão direcionadas à realização dos objetivos. Sem dúvida, entre os perfis de organizações eficazmente controladas, é provável que a maioria delas seja regularmente notificada de seu avanço no cumprimento de seus objetivos estratégicos e operacionais, bem como atinja regularmente os seus objetivos de *compliance* e produza consistentemente – período após período, ano após ano – informações confiáveis. Contudo, poderá ocorrer um evento incontrolável, uma falha ou um incidente de comunicação inadequada. Em outras palavras, até mesmo um gerenciamento de riscos corporativos eficaz pode experimentar um fracasso. Garantia razoável não é garantia absoluta.

Julgamento

A eficácia do gerenciamento de riscos corporativos sofre limitações das realidades da fraqueza humana durante tomada de decisões de negócios. As decisões devem ser tomadas por meio de julgamento humano, no tempo disponível, com base nas informações disponíveis e sob as pressões de se conduzir um negócio. Com a “clarividência” obtida da análise retrospectiva, pode-se constatar posteriormente que algumas decisões deixaram a desejar em termos de resultados desejáveis, e necessitam ser mudadas.

Colapsos

Até um gerenciamento de riscos corporativos eficaz está sujeito a um colapso. É possível que os empregados não entendam as instruções adequadamente e cometam erros de julgamento ou em decorrência de falta de atenção, distração ou cansaço. O supervisor do departamento de contabilidade, responsável pela investigação de exceções, pode simplesmente se esquecer de fazer o acompanhamento ou abandonar a investigação antes que possa efetuar as correções adequadas. Empregados temporários, que executam as tarefas de controles para empregados ausentes por motivo de férias ou doença, podem não fazê-las corretamente. Mudanças de sistema podem ser implementadas antes do pessoal ter sido treinado para responder adequadamente aos sintomas de funcionamento incorreto.

Conluio

Atividades de conluio de duas ou mais pessoas podem levar o gerenciamento de riscos corporativos ao fracasso. Indivíduos que atuam em conjunto para perpetrar e ocultar um ato, a fim de que não seja detectado, geralmente são capazes de alterar dados financeiros ou outras informações administrativas de tal forma que essas modificações não são identificadas pelo processo de gestão dos riscos corporativos. Por exemplo, um empregado que desempenha uma importante função de controle poderá agir em conluio com um cliente, fornecedor ou outro empregado. Em um nível diferente, várias camadas da gerência de vendas ou de divisão podem agir em conluio para neutralizar os controles e fazer que os resultados informados atendam a orçamentos ou cumpram metas de incentivo.

Custo-benefício

Como já discutimos no capítulo *Avaliação de Risco*, em decorrência das sempre existentes limitações de recursos, as organizações devem considerar os custos e os benefícios relativos das decisões, inclusive os relacionados à resposta aos riscos e às atividades de controle.

Ao se determinar se uma certa ação deve ser conduzida ou se um controle deve ser estabelecido, o risco de falha e o efeito em potencial sobre a organização são considerados com os custos pertinentes. Por exemplo, pode não valer a pena uma Companhia instalar controles sofisticados de estoques para monitorar níveis de matérias-primas, quando a sua representatividade no custo do processo de produção for reduzida, se a matéria-prima não for perecível, se existirem fontes disponíveis para fornecimento imediato e se o espaço de armazenamento estiver disponível.

Os custos e os benefícios da implementação de funcionalidades de identificação de eventos, avaliação de riscos, atividades pertinentes de resposta e controle são mensurados com diferentes níveis de precisão, que variam freqüentemente dependendo da natureza da organização. A questão é encontrar um ponto de equilíbrio. Da mesma forma que recursos, por serem limitados, não devem ser alocados a riscos não significativos, o controle excessivo é dispendioso e contraproducente. O cliente que faz um pedido por telefone não se submeterá a procedimentos de aprovação de pedido demasiado incômodos ou prolongados. Um banco não fará empréstimos se impuser condições em demasia a potenciais tomadores com bons antecedentes de crédito. Por outro lado, a falta de controle acarreta riscos desnecessários de inadimplência. É necessário um equilíbrio adequado em um ambiente altamente competitivo, e, apesar do despeito das dificuldades, as decisões de custo-benefício continuarão a ser feitas.

Neutralização pela Direção

O gerenciamento de riscos corporativos será tão eficaz quanto as pessoas que respondem pelo seu funcionamento. Um diretor ainda pode neutralizar o gerenciamento de riscos mesmo nas organizações dotadas de gerenciamento de riscos corporativos eficaz – aquelas que desfrutam de elevados níveis de integridade e de consciência de riscos e controle, canais de comunicação alternativos e uma diretoria ativa e bem informada, que dispõe de um processo adequado de administração. Não existe sistema de controle ou de gestão infalível, e, por isso pessoas com intenções criminosas tentarão paralisar os sistemas. Todavia, um gerenciamento de riscos corporativos eficaz melhorará a capacidade da organização de prevenir e detectar atividades de neutralização.

A frase “neutralização pela direção” é utilizada aqui com o significado de neutralizar políticas ou procedimentos recomendados para fins ilegítimos – como vantagens pessoais ou apresentação realçada das condições financeiras de uma organização ou de sua situação de compliance. O gerente de uma divisão ou unidade, ou um membro da diretoria executiva, poderá neutralizar o gerenciamento de riscos corporativos por inúmeros motivos: para aumentar a receita informada, a fim de cobrir uma redução inesperada na participação de mercado; para aumentar o valor das receitas informadas com o propósito de atender a orçamentos não realistas; aumentar o valor de mercado da Companhia antes de uma oferta pública de ações ou venda; para atender a projeções de vendas ou de receitas e justificar o pagamento de bonificações vinculadas ao desempenho ou ao valor de opções de compra de ações; ocultar violações de cláusulas em contratos de financiamento; ou ocultar o descumprimento de exigências legais. As práticas de neutralização incluem falsas declarações a banqueiros, advogados, auditores e vendedores, e emissão intencional de documentos falsos, como pedidos de compra e faturas de vendas.

A frase “neutralização pela direção” não deve ser confundida com intervenção da direção, que representa as medidas adotadas pela direção executiva para desviar-se, por motivos legítimos, de políticas ou procedimentos preestabelecidos. A intervenção da administração é necessária para se lidar com transações ou eventos não recorrentes e incomuns que, de outra forma, poderiam ser tratados inadequadamente. Os mecanismos de intervenção da alta administração são necessários porque nenhum processo pode ser formulado com o intuito de se antecipar todos os riscos ou todas as condições. De um modo geral, as medidas de intervenção da direção executiva são abertas e, normalmente documentadas ou reveladas ao pessoal apropriado. As medidas de neutralização geralmente não são nem documentadas, nem reveladas, pois há a intenção de mantê-las ocultas.

12. O Que Fazer

As medidas que podem ser adotas em decorrência deste relatório dependem da posição e da função das partes envolvidas.

- Membros do Conselho de administração – os membros do conselho devem discutir com a direção executiva a situação do gerenciamento de riscos corporativos e supervisioná-los, quando necessário. A diretoria também deve assegurar-se que os mecanismos de gerenciamento de riscos corporativos da organização funcionem com uma avaliação dos riscos mais significativos em relação à estratégia e aos objetivos, inclusive no que diz respeito às medidas que a administração está adotando e de que forma o sistema se enquadra no monitoramento do gerenciamento de riscos corporativos. O conselho deve colher informações dos auditores internos, externos e consultores.

- Diretoria executiva – este estudo sugere que o presidente deve avaliar as funcionalidades do processo de gestão de riscos corporativos. Por meio dessa estrutura, o presidente, em conjunto com os principais executivos operacionais e financeiros, pode concentrar sua atenção nos pontos necessários. Segundo a abordagem, o presidente reúne as chefias das unidades de negócios e o pessoal-chave funcional para discutir a avaliação inicial das funcionalidades e da eficácia do gerenciamento de riscos corporativos. Independentemente de seu formato, essa avaliação deve determinar se realmente existe essa necessidade e como prosseguir com uma avaliação de caráter mais amplo e mais profundo. A referida avaliação também deve assegurar que os processos de monitoramento contínuo foram implementados. O tempo despendido na avaliação do gerenciamento de riscos corporativos representa um investimento capaz de oferecer um elevado retorno.

- Empregados da Organização – os gerentes e demais empregados devem considerar que suas responsabilidades no gerenciamento de riscos corporativos estão sendo conduzidas à luz da presente estrutura, e discutir com a alta administração (Conselho de administração e diretoria executiva) idéias que possam fortalecer o processo de gestão de riscos. Cabe aos auditores internos considerar a amplitude de seu enfoque no gerenciamento de riscos corporativos.

- Órgãos reguladores – as expectativas sobre o gerenciamento de riscos corporativos variam grandemente em relação ao que este pode alcançar e ao significado do conceito de “garantia razoável” e de como deve ser aplicado. Essa estrutura possibilita uma visão compartilhada de gerenciamento de riscos corporativos, inclusive daquilo que pode fazer e de suas limitações. Os órgãos reguladores podem consultar essa estrutura ao estabelecer expectativas, por norma ou por orientação, ou ao conduzir inspeções nas organizações que supervisionam.

- Associações Profissionais – as organizações normativas e outras entidades profissionais que fornecem orientações a respeito de administração financeira, auditoria e tópicos relacionados devem considerar os seus padrões e orientações à luz da presente estrutura. A eliminação da diversidade de conceitos e da terminologia será vantajosa para todas as partes.

- Educadores - essa estrutura pode ser tema de pesquisa e análise acadêmicas, para se identificar pontos que podem receber otimizações futuras. Supondo-se que este relatório seja aceito como base comum de entendimento, seus conceitos e termos devem passar a fazer parte dos currículos universitários.

Acreditamos que este relatório ofereça inúmeros benefícios. Mediante a fundação para entendimento mútuo, todos poderão falar uma linguagem comum e comunicar-se com maior eficácia. Os executivos terão condições de analisar os processos de gerenciamento de riscos corporativos em comparação com um padrão, fortalecer o processo e conduzir suas organizações na direção das metas estabelecidas. A pesquisa futura poderá ser alavancada por uma base sólida. Os legisladores e órgãos reguladores poderão obter melhor entendimento do gerenciamento de riscos corporativos, seus benefícios e suas limitações. Se todos utilizarem uma estrutura comum de gerenciamento de riscos corporativos, os benefícios coletivos serão alcançados.

A. Objetivos e Metodologia

Em meados de 2001, o *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) iniciou um estudo com o intuito de ajudar as organizações a gerenciar riscos. Apesar da vasta literatura sobre o tema, o COSO concluiu que seria necessário que esse estudo formulasse e construísse estrutura e técnicas de aplicação relacionadas. A PricewaterhouseCoopers foi contratada para conduzir o projeto, que culminou no presente relatório, “Gerenciamento de Riscos Corporativos – Estrutura Integrada”.

O volume “Estrutura” define risco e gerenciamento de riscos corporativos e fornece definições básicas, conceitos, categorias de objetivos e componentes e princípios para se estabelecer uma estrutura completa de gerenciamento de riscos corporativos. Oferece, também, instruções para Companhias e outras organizações para determinarem como otimizar seu gerenciamento de riscos corporativos, fornecendo contexto para isso e facilitando a sua aplicação no mundo real. O presente documento também destina-se a servir de base para que uma organização determine se o seu gerenciamento de riscos corporativos é eficaz e, caso contrário, o que necessita para torná-lo eficaz.

O volume “Técnicas de Aplicação” está diretamente associado à “Estrutura” e apresenta ilustrações de técnicas de gerenciamento de riscos que Companhias e outras organizações podem implementar em vários níveis – corporativo, linha de negócios, processo ou função – e usar como apoio ao aprimoramento pontual ou evolutivo.

Como os leitores possuem diferentes necessidades, foram obtidas informações de executivos corporativos de organizações de diversos tamanhos, até mesmo de Companhias abertas e fechadas, e de diferentes setores e organizações do governo. Os executivos incluíram presidentes, executivos financeiros, executivos de riscos, *controllers*, auditores internos, legisladores, agentes normativos, advogados, auditores externos, consultores, acadêmicos e outros.

Ao longo de todo o projeto, a equipe recebeu assessoria e consultoria de um Conselho Consultivo do COSO. esse conselho, formado por altos executivos de gestão financeira, auditoria interna e externa e acadêmicos, reunia-se periodicamente com a equipe de projeto e com os membros do Conselho do COSO para revisar o plano do projeto, o andamento e os esboços da estrutura e analisar os assuntos relacionados. Quando havia registros importantes, o Conselho Consultivo e a equipe de projetos comunicavam-se com o Conselho do COSO.

A metodologia empregada neste estudo foi formulada com o intuito de proporcionar um relatório para a realização dos objetivos estabelecidos. O projeto constituiu-se de cinco fases:

I. Avaliação

A equipe de projeto avaliou a situação atual dos modelos de gerenciamento de riscos mediante análise da literatura, pesquisas e seminários com a finalidade de colher informações relevantes sobre todo o espectro de gerenciamento de riscos. Nessa fase, analisaram-se as informações, comparando e contrastando conceitos, práticas das filosofias e protocolos de gerenciamento de riscos, entendimento das necessidades dos usuários e identificação de questões e problemas críticos.

II. Concepção

A equipe criou um modelo conceitual da estrutura de gerenciamento de riscos corporativos e desenvolveu um conjunto preliminar de ferramentas como base para as técnicas de aplicação. Empregando técnicas personalizadas de solicitação de informações, a equipe testou os conceitos com os principais grupos de usuários e de *stakeholders* e, com base no *feedback*, refinou o modelo conceitual.

III. Construção e Design

Com base no modelo conceitual refinado, a equipe desenvolveu a estrutura, inclusive as definições, as categorias de objetivos, os componentes, os princípios, a infra-estrutura e o contexto gerencial, ao longo das respectivas discussões. Essa fase também compreendeu a formulação da organização e a abordagem para o desenvolvimento das técnicas de aplicação. Para contemplar as reações e obter sugestões de melhoria, o esboço da estrutura e o desenho das técnicas de aplicação foram revisados, em conjunto, com os principais usuários e *stakeholders*.

IV. Preparação para Exposição Pública

Nessa fase, a equipe refinou a estrutura e desenvolveu, mais ainda, as técnicas de aplicação, revisando-as com executivos de diversas organizações, que forneceram *feedback* sobre seu valor e sua utilidade.

V. Finalização

Essa fase compreendeu a exposição pública do volume sobre Estrutura por um período de 90 dias, durante o qual foram colhidos comentários e realizados testes de campo da estrutura em organizações selecionadas. Após o recebimento dos comentários, a equipe de projetos os revisou e analisou para identificar as modificações necessárias. A equipe concluiu os volumes de Estrutura e “Aplicações Técnicas”, e forneceu os manuscritos finais ao conselho do COSO e seu Conselho Consultivo, para análise e aprovação.

Como parte desse processo, a equipe de projeto considerou cuidadosamente todas as informações recebidas, incluindo outras estruturas já existentes. O “Apêndice D – Bibliografia Selecionada” apresenta uma lista de algumas das publicações utilizadas como referência. Como seria de se esperar, muitas opiniões diferentes e, às vezes, contraditórias foram manifestadas quanto às questões fundamentais – em uma certa fase do projeto ou entre elas. A equipe de projetos, sob a supervisão do Conselho e do Conselho Consultivo do COSO, considerou cuidadosamente os méritos das posições manifestadas em caráter individual e no contexto das questões relacionadas, adotando aquelas que facilitavam o desenvolvimento de uma estrutura relevante, lógica e internamente consistente. O Conselho Consultivo do COSO e a diretoria ofereceram seu total apoio, e aprovaram a estrutura resultante do processo.

B. Resumo dos Princípios Fundamentais

A seguir, destacam-se os princípios fundamentais dos oito componentes de gerenciamento de riscos. Este apêndice não pretende descrever os princípios estabelecidos na “Estrutura”, nem precisamente ou em sua totalidade, nem representar uma lista completa de princípios.

Ambiente Interno

Filosofia de Gerenciamento de Riscos

- A filosofia de gerenciamento de riscos de uma organização representa as convicções e as atitudes compartilhadas, o que caracteriza a maneira pela qual essa organização considera o risco em todas as suas atividades.
- Reflete os valores da organização, influenciando sua cultura e estilo operacional.
- Tem efeito sobre o modo pelo qual os componentes do gerenciamento de riscos corporativos são aplicados, inclusive como os eventos são identificados, os tipos de riscos aceitos e a forma como são administrados.
- Deve estar bem desenvolvida, entendida e apoiada pelo pessoal da organização.
- Deve ser observada nas declarações das políticas, comunicações escritas e orais, e no processo decisório.
- A administração reforça a filosofia não apenas verbalmente, mas por meio de suas ações do dia-a-dia.

Apetite a riscos

- O apetite a riscos da organização reflete a sua filosofia de gerenciamento de riscos, influencia a cultura e o estilo operacional.
- É considerado no estabelecimento da estratégia, que deve estar alinhada ao apetite a riscos.

Conselho de Administração

- A diretoria é ativa e tem um grau adequado de conhecimentos de gestão, técnicos e outras especialidades, aliados à atitude necessária para executar suas responsabilidades de supervisão.
- Está preparada para questionar e apurar as atividades da gestão, apresentar opiniões alternativas e agir no caso de atos ilícitos.
- Constituído, ao menos, por maioria de conselheiros externos e independentes à organização.
- Fornece supervisão ao gerenciamento de riscos corporativos, está ciente e concorda com o apetite a riscos da organização.

Integridade e Valores Éticos

- Os padrões de comportamento da organização refletem integridade e valores éticos.
- Os valores éticos não são apenas comunicados, mas também acompanhados por meio de orientação explícita sobre o que está certo ou errado.
- A integridade e os valores éticos são comunicados por intermédio de um código de conduta formal.
- Existem canais ascendentes de comunicação pelos quais os empregados sentem-se confortáveis em trazer informações pertinentes.
- São aplicadas penalidades aos empregados que transgridem o código; determinados mecanismos incentivam o empregado a denunciar suspeitas de infração e medidas disciplinares são adotadas contra os que deixam de relatá-las.
- A integridade e os valores éticos são transmitidos pelas ações da alta administração e seus exemplos.

Compromisso com a Competência

- A competência dos empregados da organização reflete o conhecimento e as habilidades necessárias para a execução das tarefas designadas.
- A administração alinha competência ao custo.

Estrutura Organizacional

- A estrutura organizacional define as áreas fundamentais de responsabilidade.
- Estabelece as linhas de comunicação.
- É desenvolvida de acordo com o tamanho da organização e a natureza de suas atividades.
- Possibilita um gerenciamento de riscos eficaz.

Atribuição de Autoridade e de Responsabilidade

- A atribuição de autoridade e de responsabilidade estabelece até que ponto pessoas ou equipes estão autorizadas, e são incentivadas, a fazer uso de sua iniciativa para tratar de questões e resolver problemas, e estabelece limites de autoridade.
- As atribuições estabelecem relacionamentos de comunicação e protocolos de autorização.
- As políticas descrevem as práticas comerciais apropriadas, o conhecimento e a experiência do pessoal-chave, bem como os recursos associados.
- Cada indivíduo sabe como as suas ações inter-relacionam-se e contribuem para a realização dos objetivos.

Normas de Recursos Humanos

- As normas tratam de admissão, orientação, treinamento, avaliação, aconselhamento, promoção, compensação e medidas corretivas, conduzindo os níveis previstos de integridade, de comportamento ético e de competência.
- As medidas disciplinares transmitem a mensagem de que as infrações ao comportamento esperado não serão toleradas.

Fixação de Objetivos

Objetivos Estratégicos

- Os objetivos estratégicos da organização estabelecem metas em nível elevado que se alinham e dão suporte à sua missão/visão.
- Refletem as escolhas estratégicas da administração e o modo pelo qual a organização tentará gerar valor para as partes interessadas.
- A administração identifica os riscos associados às escolhas estratégicas e considera as suas implicações.

Objetivos Correlatos

- Os objetivos correlatos dão suporte à estratégia escolhida e são alinhados a ela; são relativos a todas as atividades da organização.
- Cada nível de objetivos está associado aos objetivos mais específicos, que fluem em cascata pela organização.
- Os objetivos são facilmente entendidos e mensurados.
- Alinham-se ao apetite a risco.

Objetivos Selecionados

- A administração dispõe de um processo que alinha os objetivos estratégicos com a missão da organização e assegura que os objetivos estratégicos e correlatos tenham relação com seu apetite a riscos.

Apetite a Riscos

- O apetite a riscos da organização serve de guia para se fixar estratégias.
- Orienta a alocação de recursos.
- Alinha a organização, o pessoal, os processos e a infra-estrutura.

Tolerância a Riscos

- As tolerâncias a riscos são mensuráveis, de preferência, nas mesmas unidades que os objetivos correlatos.
- Alinham-se ao apetite a riscos.

Identificação de Eventos

Eventos

- A administração identifica os eventos em potencial capazes de afetar a implementação da estratégia ou a realização dos objetivos – aqueles que podem provocar impacto positivo ou negativo, ou ambos.
- Mesmo os eventos de possibilidade relativamente reduzida de ocorrência são considerados se o impacto sobre a realização de um objetivo importante for significativo.

Fatores Influenciadores

- A administração reconhece a importância de se entenderem os fatores externos e internos e o tipo de eventos gerado por eles.
- Os eventos são identificados no âmbito da organização e da atividade.

Técnicas de Identificação de Eventos

- Técnicas utilizadas para examinar o passado e o futuro.
- A administração seleciona técnicas que se ajustam à filosofia de gerenciamento de riscos e assegura que a organização desenvolve as funcionalidades necessárias à identificação de eventos.
- A identificação de eventos é um sistema complexo, que constitui a base para os componentes de avaliação e de resposta a riscos.

Interdependências

- A administração entende o modo pelo qual os eventos se relacionam.

Diferenciação entre Riscos e Oportunidades

- Os eventos capazes de causar impacto negativo representam riscos, os quais a administração avalia e gera uma resposta.
- Os eventos que representam oportunidades são canalizados de volta aos processos de fixação de objetivos ou da estratégia da organização.

Avaliação de Riscos

- Ao avaliar riscos, a administração considera os eventos previstos e imprevistos.

Risco Inerente e Risco Residual

- A administração avalia os riscos inerentes.
- Após o desenvolvimento das respostas aos riscos, a administração passa a considerar o risco residual.

Estimativa da Probabilidade e do Impacto

- Os eventos em potencial são avaliados com base em duas perspectivas: probabilidade e impacto.
- Ao avaliar o impacto, a administração geralmente aplica a mesma unidade compatível de medida que a utilizada para o objetivo.
- O horizonte de tempo para se avaliar riscos deve ter relação com o horizonte de tempo da estratégia correlata e dos objetivos.

Técnicas de Avaliação

- A administração emprega uma combinação de técnicas qualitativas e quantitativas.
- As técnicas dão suporte ao desenvolvimento de uma avaliação combinada de riscos.

Relações entre Eventos

- Nos casos em que existe correlação entre eventos, ou em que os eventos se combinam e interagem, a administração os avalia em conjunto.

Resposta a Riscos

- Ao responder ao risco, a administração considera se deverá evitá-lo, reduzi-lo, compartilhá-lo ou aceitá-lo.

Avaliação das Possíveis Respostas

- As respostas são avaliadas com a finalidade de se alinhar o risco residual às tolerâncias aos riscos.
- Ao avaliar as respostas a riscos, a administração considera seus efeitos sobre a probabilidade e o impacto.
- A administração considera os custos em relação aos benefícios e às novas oportunidades.

Respostas Selecionadas

- As respostas selecionadas pela administração são formuladas para levar a probabilidade de risco e o seu impacto a níveis compatíveis com as tolerâncias a riscos.
- A administração considera os riscos adicionais que podem surgir de uma resposta.

Visão em Portfólio

- A administração considera o risco com base na perspectiva de toda a organização ou em uma visão de portfólio.
- A administração determina se o perfil de risco residual da organização é proporcional ao seu apetite a riscos.

Atividades de Controle

Integração com a Resposta a Riscos

- A administração identifica as atividades de controle necessárias para assegurar que as respostas a riscos sejam conduzidas de maneira adequada e oportunamente.
- A seleção ou a revisão das atividades de controle incluem a consideração de sua pertinência e a adequação às respostas aos riscos e ao objetivo correlato.
- Ao selecionar as atividades de controle, a administração considera o modo pelo qual as atividades de controle se inter-relacionam.

Tipos de Atividades de Controle

- A administração escolhe com base numa variedade de atividades de controle, até mesmo atividades preventivas, de detecção, manuais, informatizadas e administrativas.

Políticas e Procedimentos

- As políticas são implementadas ponderada, conscienciosa e consistentemente.
- Os procedimentos são executados com um enfoque nítido e continuado das condições às quais a política é direcionada.
- As condições identificadas em decorrência do procedimento são investigadas, e medidas corretivas apropriadas são adotadas.

Controles de Sistemas de Informações

- Implementam-se os controles apropriados: gerais e para aplicações.

Informação e Comunicação

Informações

- Informações pertinentes são obtidas de fontes internas e externas.
- A organização colhe e utiliza os dados históricos e atuais necessários para o apoio adequado ao gerenciamento de riscos corporativos.
- A infra-estrutura de informações converte os dados puros em informações pertinentes, que ajudarão os empregados a incumbir-se de suas responsabilidades de gerenciamento de riscos corporativos e de outras responsabilidades; as informações são fornecidas na profundidade, forma e no prazo, que as tornam acionáveis, imediatamente utilizáveis e vinculadas a responsabilidades definidas, inclusive as relacionadas à necessidade de identificar, avaliar e responder ao risco.
- Os dados-fonte e as informações são confiáveis e fornecidos oportunamente e no local adequado, a fim de possibilitar um processo decisório eficaz.
- A pontualidade do fluxo de informações é consistente com o índice de mudança nos ambientes interno e externo da organização.
- Os sistemas de informações mudam sempre que necessário, para que possam dar suporte aos novos objetivos.

Comunicações

- A administração fornece comunicação específica e dirigida, abordando expectativas do comportamento e das responsabilidades do pessoal, inclusive uma declaração transparente da filosofia de gerenciamento de riscos da organização, abordagem, e clara delegação de autoridade.

- A comunicação sobre processos e procedimentos, sustenta e está alinhada à cultura desejada.
- Todo o pessoal recebe uma mensagem claramente delineada da alta administração, de que o gerenciamento de riscos corporativos deve ser levado a sério.
- O pessoal sabe como suas atividades relacionam-se com o trabalho dos outros, o que os capacita a reconhecer problemas, determinar a causa e adotar medidas corretivas.
- O pessoal sabe o que é considerado comportamento aceitável e inaceitável.
- Existem canais abertos de comunicação e disposição de ouvir, e o pessoal acredita que seus superiores realmente desejam conhecer os problemas e tratá-los com eficácia.
- Existem canais de comunicação fora dos costumeiros, e o pessoal entende que não haverá represália à comunicação de informações relevantes.
- Existem canais de comunicação abertos entre o conselho de administração e a diretoria executiva, em que as informações adequadas são comunicadas oportunamente.
- Existem canais de comunicação abertos a clientes e fornecedores, que podem oferecer informações significativas.
- A empresa transmite informações relevantes a órgãos reguladores, analistas financeiros e outras partes externas.

Monitoramento

- A administração determina, por meio de atividades contínuas de monitoramento ou avaliações independentes, ou por uma combinação dessas, se o gerenciamento de riscos corporativos atual continua eficaz.

Atividades Contínuas de Monitoramento

- As atividades de monitoramento são incorporadas às operações normais e recorrentes da organização, realizadas no decurso natural dos negócios.
- São conduzidas em tempo real e reagem dinamicamente a condições em fase de transição.

Avaliações Independentes

- As avaliações separadas enfocam diretamente a eficácia do gerenciamento de riscos corporativos e oferecem oportunidade de considerar a manutenção da eficácia das atividades contínuas de monitoramento.
- O avaliador entende cada uma das atividades da organização e cada um dos componentes de gerenciamento de riscos corporativos que está sendo abordado.
- O avaliador analisa o desenho do processo de gestão de riscos corporativos e os resultados dos testes executados, comparados com as normas estabelecidas pela administração, e determina se o gerenciamento de riscos corporativos oferece uma garantia razoável referente aos objetivos definidos.

Relato de Deficiências

- As deficiências relatadas a partir de fontes internas e externas são consideradas cuidadosamente por suas implicações para o gerenciamento de riscos corporativos, e medidas corretivas apropriadas são adotadas.
- Todas as deficiências identificadas, capazes de afetar a capacidade da organização de desenvolver e implementar a sua estratégia e realizar seus objetivos preestabelecidos, são relatadas às pessoas com condições de adotar as medidas necessárias.
- Não apenas as transações ou os eventos relatados são investigados e corrigidos, mas também os procedimentos subjacentes potencialmente falhos também são reavaliados.
- São estabelecidos protocolos para se identificar as informações necessárias em um certo nível para um processo decisório mais eficaz.

Funções e Responsabilidades

Conselho de Administração

- O Conselho tem conhecimento que ponto a administração estabeleceu, na organização, um gerenciamento de riscos corporativos eficaz.
- Está ciente e concorda com o apetite a riscos.
- Analisa a visão de portfólio dos riscos contrastantes com o apetite a riscos.
- É informada dos riscos mais significativos e sobre a administração, se está ou não respondendo adequadamente.

Administração

- Cabe ao presidente a responsabilidade final pelo gerenciamento de riscos corporativos.
- O presidente assegura que o ambiente interno é positivo e que todos os componentes de gerenciamento de riscos corporativos estão implementados.
- Os gerentes de alto nível, encarregados das unidades organizacionais, são responsáveis pelo gerenciamento dos riscos relacionados aos objetivos de suas unidades.
- Orientam a aplicação do gerenciamento de riscos corporativos, assegurando-se de que essa aplicação é consistente com a tolerância a risco.
- Todo gestor é responsável, perante o nível imediatamente superior, por sua parcela de gerenciamento de riscos corporativos, cabendo ao presidente a responsabilidade final ante o conselho.

Demais Funcionários da Organização

- O gerenciamento de riscos corporativos faz parte explícita ou implícita da descrição de cargo de todo empregado.
- O pessoal está ciente da necessidade de resistir à pressão de superiores para participar de atividades ilícitas e da disponibilidade de canais de comunicação fora das linhas normais, para possibilitar o relato dessas circunstâncias.
- As funções e responsabilidades de todo o pessoal pelo gerenciamento de riscos corporativos estão nitidamente definidas e comunicadas adequadamente.

Partes que Interagem com a Organização

- Os mecanismos já estão implementados para receber informações pertinentes das partes que interagem com a empresa e adotar as medidas cabíveis.
- As medidas não se limitam a resolver apenas uma situação específica relatada, mas também a investigar a fonte subjacente do problema e corrigi-la.
- A administração implementou um programa para monitorar as atividades terceirizadas.
- A administração leva em conta as observações e os *insights* de analistas financeiros, agências de rating e da mídia jornalística, que podem otimizar o gerenciamento de riscos corporativos.

C. Relação Entre Gerenciamento de Riscos Corporativos - Estrutura Integrada e Controle Interno - Estrutura Integrada

Em 1992, o "*Committee of Sponsoring Organizations of the Treadway Commission*" publicou o "*Internal Control – Integrated Framework*", que estabelece uma estrutura de controles internos e fornece ferramentas de avaliação para uso de empresas e de outras entidades para avaliar seus sistemas de controle. A estrutura identifica e descreve cinco componentes inter-relacionados e necessários para um controle interno eficaz.

O "*Internal Control – Integrated Framework*" define o controle interno como um processo conduzido pelo conselho de administração, pela administração e pelo corpo de empregados de uma organização, com a finalidade de possibilitar uma garantia razoável quanto à realização dos objetivos nas seguintes categorias:

- Eficácia e eficiência das operações;
- Confiabilidade das demonstrações financeiras;
- Conformidade com leis e regulamentos cabíveis.

Este apêndice esboça a relação entre a estrutura de controle interno e a estrutura do gerenciamento de riscos corporativos.

Mais Amplo que Controle Interno

O controle interno está situado no centro, e faz parte integral do gerenciamento de riscos corporativos. Esse gerenciamento é de caráter mais amplo do que o controle interno, expandindo e acrescentando detalhes ao controle interno para formar uma conceituação mais robusta e totalmente focada em risco. O "*Internal Control – Integrated Framework*" permanece implementado para empresas e outras organizações que procuram apenas o controle interno isolado.

Categorias de Objetivos

O "*Internal Control – Integrated Framework*" especifica três categorias de objetivos: operacionais, relatórios financeiros e compliance. O gerenciamento de riscos corporativos especifica três categorias de objetivos semelhantes: operacionais, de comunicação e de *compliance*. A categoria de comunicações na estrutura de controle interno relaciona-se com a confiabilidade das demonstrações financeiras publicadas. Na estrutura do gerenciamento de riscos corporativos, a categoria de comunicação foi expandida significativamente, a fim de envolver todos os relatórios desenvolvidos pela organização, divulgados tanto interna quanto externamente. Essa categoria inclui os relatórios utilizados internamente

pela administração e os publicados para partes externas, inclusive arquivamentos obrigatórios e relatórios a outros *stakeholders*. Além disso, seu alcance estende-se, partindo da situação financeira, mas não se limitando a cobrir as informações financeiras em um caráter mais amplo, mas também as informações não financeiras.

O "Gerenciamento de Riscos Corporativos – Estrutura Integrada" adiciona outra categoria de objetivos, ou seja, objetivos estratégicos, que atuam em um nível mais elevado que os outros. Os objetivos estratégicos fluem da missão ou da visão da organização, enquanto os objetivos operacionais, de comunicação e de compliance devem estar alinhados a eles. O gerenciamento de riscos corporativos é aplicado para se definir a estratégia, assim como nas ações para que esses objetivos sejam alcançados nas outras três categorias.

A estrutura de gerenciamento de riscos corporativos introduz os conceitos de apetite a riscos e a tolerância a risco. O apetite a riscos é a quantidade de risco estabelecida, de modo amplo que uma empresa está disposta a aceitar na busca de sua missão/visão. O apetite a riscos serve como ponto de referência para se fixar as estratégias e a escolha dos objetivos correlatos. As tolerâncias a riscos são os níveis aceitáveis de variação referentes à realização dos objetivos. Ao fixar as tolerâncias a riscos, a administração analisa a importância relativa dos objetivos correlatos e alinha as tolerâncias com o apetite a riscos. A utilização de tolerâncias a riscos propicia à administração maior garantia de que a organização permanece dentro de seu apetite a riscos, o qual, por sua vez, possibilita maior grau de conforto de que a empresa realizará os seus objetivos.

Visão de Portfólio

Um conceito não contemplado na estrutura de controle interno é a visão de portfólio dos riscos, que, além de se concentrar nos riscos ao se analisar o cumprimento de cada um dos objetivos da organização, leva em conta os riscos combinados em uma visão de carteira.

Componentes

Com maior enfoque em risco, a estrutura de gerenciamento de riscos corporativos amplia o componente de gerenciamento de riscos da estrutura de controle interno, criando quatro componentes: fixação de objetivos (que é um pré-requisito do controle interno), identificação de eventos, avaliação de riscos e resposta a riscos.

Ambiente Interno

Ao abordar o ambiente, a estrutura de gerenciamento de riscos corporativos discute uma filosofia de vinculada a esse gerenciamento, a qual é um conjunto de convicções e atitudes compartilhadas, que caracterizam a forma por meio da qual a organização considera os riscos, refletindo os seus valores e influenciando sua cultura e estilo operacional. Como já descrevemos anteriormente, a estrutura compreende o conceito do apetite a riscos, que é mantido mediante tolerâncias a riscos mais específicas.

Em vista da importância crítica do conselho de administração e de sua composição, a estrutura de gerenciamento de riscos corporativos amplia o requisito da estrutura de controle interno para pelo menos uma massa crítica de diretores independentes - isto é, normalmente um mínimo de dois diretores independentes – e afirma que, para que o gerenciamento de riscos corporativos possa ser eficaz, o conselho deverá possuir, pelo menos em sua maioria constituída, conselheiros externos independentes.

Identificação de Eventos

As estruturas de gerenciamento de riscos corporativos e de controle interno reconhecem que os riscos podem ocorrer em qualquer nível da organização, bem como ser originados de uma variedade de fatores internos e externos. Assim, ambas as estruturas consideram a identificação de riscos no contexto do potencial de impacto sobre a realização dos objetivos.

A estrutura de gerenciamento de riscos corporativos aborda o conceito de eventos em potencial, definindo um evento como um incidente ou uma ocorrência gerada por fontes internas ou externas, que afetam a implementação da estratégia ou a realização dos objetivos. Os eventos em potencial cujo impacto é positivo representam oportunidades, enquanto os de impacto negativo representam riscos. O gerenciamento de riscos corporativos requer a identificação desses eventos em potencial, utilizando uma combinação de técnicas que examinam tendências passadas e emergentes, capazes de desencadear eventos.

Avaliação de Riscos

Enquanto a estrutura de controle interno e a do gerenciamento de riscos corporativos requerem a avaliação de riscos em termos de sua probabilidade de ocorrência e impacto potencial, a estrutura de gerenciamento de riscos corporativos recomenda a avaliação de riscos por meio de uma lente mais poderosa. Os riscos são considerados inerentes e, sob o aspecto residual, expressos de preferência na mesma unidade de mensuração que a usada para os objetivos aos quais os riscos se relacionam. Os horizontes de tempo devem ser consistentes com as estratégias, com os objetivos da organização e, se possível, com os dados observáveis. A estrutura de gerenciamento de riscos corporativos também chama a atenção para os riscos inter-relacionados, descrevendo como um único evento poderá gerar diversos riscos.

Como foi observado, o gerenciamento de riscos corporativos considera a necessidade da administração desenvolver uma visão de carteira no âmbito de toda a organização. Os gestores são os responsáveis por unidade de negócios, função, processo ou outras atividades, com o desenvolvimento de uma avaliação combinada dos riscos em relação a unidades específicas, a alta direção, no âmbito de toda a organização, analisa riscos a partir de uma perspectiva de “carteira”.

Resposta a Riscos

A estrutura de gerenciamento de riscos corporativos identifica quatro categorias de resposta a riscos: evitar, reduzir, compartilhar e aceitar. Como parte do gerenciamento de riscos corporativos, a administração considera as respostas em potencial dessas categorias e com a finalidade de obter um nível de risco residual compatível com as tolerâncias a riscos da empresa. Após considerar essas respostas a riscos, isoladamente ou em grupo, a administração avalia o efeito agregado destas em toda a organização.

Atividades de Controle

Ambas as estruturas apresentam atividades de controle para ajudar a assegurar que as respostas a riscos da administração sejam executadas. A estrutura de gerenciamento de riscos corporativos ressalta expressamente que em determinadas circunstâncias as próprias atividades de controle servem de resposta a riscos.

Informação e Comunicação

A estrutura de gerenciamento de riscos corporativos permite detalhar melhor o componente de controle interno de informações e comunicação, incentivando o exame de dados extraídos de eventos passados, presentes e futuros em potencial. Os dados históricos permitem que a organização compare o desempenho real em relação às metas, aos planos e às expectativas e possibilita *insights* sobre o desempenho da organização em períodos anteriores e em condições variadas. Dados correntes ou dados da situação atual possibilitam importantes informações adicionais; já dados sobre eventos futuros em potencial e fatores subjacentes completam a análise das informações. A infra-estrutura de informações procura e colhe dados em um período de tempo e uma profundidade de detalhes consistentes com a necessidade que a organização tem de identificar eventos, avaliá-los, responder aos riscos e manter seu apetite a riscos dentro do escopo planejado.

O debate sobre a existência de um canal de comunicação alternativo, fora das linhas normais de comunicação, na estrutura de controle interno dá mais ênfase na estrutura de gerenciamento de riscos corporativos, que afirma que um processo de gestão de riscos eficaz requer o referido canal.

Funções e Responsabilidades

Ambas as estruturas concentram-se nas funções e nas responsabilidades de várias partes que as compõem, ou fornecem informações importantes ao controle interno e ao gerenciamento de riscos corporativos. A estrutura de gerenciamento de riscos corporativos descreve a função e as responsabilidades dos responsáveis por riscos, e possibilita detalhes adicionais a respeito da função da diretoria executiva de uma organização.

D. Bibliografia Selecionada

American Institute of Certified Public Accountants and The Canadian Institute of Chartered Accountants. *Managing Risk in the New Economy*. New York. AICPA. 2000.

Banham, Russ. *A High Level of Intolerance*. CFO, The Magazine for Senior Financial Executives, April 2000.

Barton ,Thomas L., William G. Shenkir, and Paul L.Walker. Making Enterprise Risk Management Pay Off: *How Leading Companies Implement Risk Management*. Financial Executive, 2001.

Bazerman, Max H. *Judgment in Managerial Decision Making*. New York: John Wiley & Sons, 2001.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). *Internal Control – Integrated Framework*. New York: AICPA, 1992.

Crouhy, Michael, Dan Galai, and Robert Mark. *Risk Management*. New York: McGraw-Hill, 2001.

Davidson, Clive. *Lofty Ambitions for Measuring Global Risk*. Securities Industry News, June 5, 2000.

DeLoach, James W. Enterprise-Wide Risk Management: *Strategies for Linking Risk and Opportunity*. London: Financial Times Prentice Hall, 2000.

DiPiazza, Samuel A., Jr. and Robert G. Eccles. *Building Public Trust: The Future of Corporate Reporting*. New York. John Wiley & Sons. 2002.

Everson, Miles. *Creating an Operational Risk-Sensitive Culture*. The RMA Journal. March 1, 2002.

Economist Intelligence Unit in cooperation with Arthur Andersen & Co. *Managing Business Risk – An Integrated Approach*. The Economist Intelligence Unit, 1995.

Economist Intelligence Unit in cooperation with MCC Enterprise Risk. *Enterprise Risk Management – Implementing New Solutions*. The Economist Intelligence Unit, 2001.

FEI Research Foundation in cooperation with Andersen. *Risk Management: An Enterprise Perspective*. Financial Executive, 2002.

Haubenstock, Michael and John Gontero. *Operational Risk Management: The Next Frontier*. New York: RMA, 2001.

Institute of Chartered Accountants in England and Wales. *Internal Control Guidance for Directors on the Combined Code*. London: ICAEW, 1999.

Institute of Directors in Southern Africa. *King Report on Corporate Governance for South Africa 2001*. The Institute of Directors in Southern Africa, 2001.

International Organization for Standardization. *ISO/IEC Guide 73*. 2002.

Lam, James. *The CRO Is Here to Stay*. Risk Management. April 2001.

National Commission on Fraudulent Financial Reporting. *Report of the National Commission on Fraudulent Financial Reporting*, 1987.

Nottingham, Lucy. *A Conceptual Framework for Integrated Risk Management*. Ottawa: Conference Board of Canada, 1997.

Risk Management Group of the Basel Committee on Banking Supervision. *Sound Practices for the Management and Supervision of Operational Risk*, 2001.

Root, Stephen J. *Beyond COSO Internal Control to Enhance Corporate Governance*. New York: John Wiley & Sons, 1998.

Standards Australia and Standards New Zealand. *Australian/New Zealand Standard 4360:1999: Risk Management*. Standards Australia and Standards New Zealand, 1999.

Steinberg, Richard M. *The CEO and the Board: Enhancing the Relationship*. G100 Insights. April 2003.

Steinberg, Richard M. and Catherine L. Bromilow. Corporate Governance and the Board – *What Works Best*. The Institute of Internal Auditors Research Foundation, 2001.

The Institute of Risk Management (IRM), The Association of Insurance and Risk Managers (AIRMIC), and ALARM The National Forum for Risk Management in the Public Sector. *A Risk Management Standard*. AIRMIC, ALARM, and IRM, 2002.

Thiessen, Karen. *A Composite Sketch of Chief Risk Officer*. Ottawa: Conference Board of Canada, 2001.

Thiessen, Karen. *Don't Gamble with Goodwill – The Value of Effectively Communicating Risks*. Ottawa: Conference Board of Canada, 2000.

Tillinghast–Towers Perrin. *Enterprise Risk Management: Trends and Emerging Practices*. New York: Tillinghast–Towers Perrin, 2001.

Walker, Paul L., William G. Shenkir, and Thomas L. Barton. Enterprise *Risk Management: Pulling It All Together*. The Institute of Internal Auditors Research Foundation, 2002.

E. Consideração aos Comentários Recebidos

Conforme observado no Apêndice A, uma minuta deste documento sobre a estrutura foi elaborada e exposta para suscitar comentários públicos. As 78 cartas contêm centenas de comentários isolados a respeito de uma variedade de questões. Levamos em conta cada um dos comentários elaborados ao formular revisões no documento final. Este apêndice apresenta de forma resumida não apenas as questões mais significativas e as modificações resultantes que se refletem no relatório definitivo, mas também os motivos segundo os quais determinadas opiniões foram aceitas em lugar de outras.

Definição de Gerenciamento de Riscos Corporativos

Geração de Valor para as Partes Interessadas

A minuta exposta descreve como o gerenciamento de riscos corporativos permite que uma organização gere valor para às partes interessadas, embora o conceito de valor não esteja explicitamente refletido na definição de gerenciamento de riscos corporativos. Alguns dos comentários sugerem que a definição deva fazer uma referência expressa.

Concluiu-se que a definição apresentada deveria ser mantida, uma vez que afirma com clareza que o gerenciamento de riscos corporativos implica o fornecimento de assistência para atingir os objetivos da organização, os quais inerentemente geram valor. Além disso, o esboço da definição descreve como o gerenciamento de riscos corporativos gera valor às partes interessadas. Em virtude da existência dessa associação ao valor e da descrição deste, e para evitar definições exageradamente longas (como foi sugerido por outros colaboradores que enviaram os seus comentários), a definição atual foi mantida.

Oportunidades

A minuta apresentada descreve o modo como o gerenciamento de riscos corporativos requer a identificação e a abordagem a eventos em potencial que possam provocar um impacto negativo a uma organização, os quais são chamados de riscos, e os eventos de impacto positivo são denominados oportunidades. Algumas das cartas afirmavam que, em virtude da importância da identificação de oportunidades, a definição de risco deveria ser ampliada a fim de incluir esse conceito. Outros defendiam que a não inclusão das oportunidades na definição de riscos poderia induzir o leitor a não ver as oportunidades como parte do gerenciamento de riscos corporativos, enfraquecendo, desse modo, a pertinência da estrutura. Por outro lado, determinados leitores sugeriram que todas as referências às oportunidades deveriam ser eliminadas do relatório final.

Concluiu-se que, em virtude da importância de identificar e aproveitar as oportunidades, a discussão das oportunidades da estrutura deveria ser mantida e otimizada, e o relatório final ampliar a discussão de identificar e reagir às oportunidades, como parte integrante do gerenciamento de riscos corporativos. As discussões nos capítulos componentes do relatório final descrevem ainda mais o processo pelo qual a administração considera tanto os efeitos negativos quanto os positivos – ou o aspecto da oportunidade – dos eventos em potencial no gerenciamento de riscos. No que tange à definição de risco, concluiu-se que a adição do conceito de oportunidade encobriria os conceitos, dificultando ainda mais a comunicação. Manter a distinção entre um evento negativo e um positivo traz clareza à linguagem do gerenciamento de riscos corporativos.

Um Processo

A minuta apresentada ao público define o gerenciamento de riscos corporativos como um processo e, ainda, estabelece componentes que podem ser vistos como elementos deste. Alguns leitores afirmaram que o termo “processo” é inadequado, porque implica a execução de etapas ou tarefas seqüenciais.

O presente relatório foi revisado para reforçar o conceito de que o gerenciamento de riscos corporativos não é necessariamente conduzido de forma seqüencial, mas, na realidade, é uma atuação recíproca contínua e repetitiva de ações conduzidas por uma organização.

Aplicado a uma Estratégia Definida

A minuta apresentada descreve como os objetivos devem ser estabelecidos e comunicados, antes que os riscos à sua realização possam ser identificados e solucionados. Afirma-se, também, que as técnicas de gerenciamento de riscos corporativos sejam aplicadas na fixação das estratégias, para assistir à administração na avaliação e da seleção das estratégias para a organização, e da sua associação aos objetivos correlatos. Algumas pessoas comentaram que o gerenciamento de riscos é secundário ao desenvolvimento de uma estratégia para a organização elaborada pela administração, e que a estrutura gera um enfoque demasiado em riscos ao invés de na fixação de objetivos.

Concluiu-se que não é necessário nem útil retratar o conceito, a definição da estratégia como aspectos mais importantes do que o gerenciamento de riscos. Ambos são importantes e inerentes ao gerenciamento de riscos corporativos. Entretanto, o documento final contém uma discussão mais elaborada do processo de definição de estratégias e de objetivos na execução do gerenciamento de riscos corporativos.

Apetite a Riscos e Tolerâncias a Riscos

A minuta apresentada discute os conceitos de apetite a riscos e as tolerâncias a riscos. Alguns leitores sugerem que seria conveniente apresentar informações adicionais, inclusive orientação sobre como expressar e mensurar o apetite a riscos. Outros leitores afirmam que existe muito pouca diferença entre esses dois conceitos e que ambos devem ser combinados.

O relatório final mantém a diferenciação entre apetite a riscos e tolerâncias a riscos, segundo a qual o apetite a riscos pertence a um nível elevado na organização como um todo, enquanto que as tolerâncias a riscos referem-se a objetivos específicos. O volume “Técnicas de Aplicação” ilustra a aplicação desses conceitos.

Permite Garantia Razoável

Determinados leitores sugerem que o conceito de garantia razoável deve ser definido com maior exatidão.

Concluiu-se que o debate sobre o termo “garantia razoável” é adequado, porém uma maior exatidão nessa definição está além do alcance desse projeto.

Categorias de Objetivos

Determinados leitores afirmam que o estabelecimento de categorias de objetivos de uma organização não tem validade e, ainda, complica exageradamente a estrutura.

O documento final mantém a categoria de objetivos da organização, que fundamentado no motivo que a categorização possibilita um enfoque nos diferentes aspectos do gerenciamento de riscos corporativos, facilita a diferenciação entre aquilo que pode ser esperado de cada categoria de objetivos e incentiva a utilização de uma linguagem comum para o gerenciamento de riscos corporativos.

Realização dos Objetivos

Alguns leitores questionam o motivo segundo o qual a “garantia razoável” é somente aplicada ao ponto até o qual os objetivos estratégicos e operacionais estão sendo realizados em vez de aplicada à sua realização efetiva.

Concluiu-se que a diferenciação entre aquilo que pode ser esperado do gerenciamento de riscos corporativos quanto ao cumprimento dos objetivos estratégicos e operacionais, de comunicação e de compliance, continua a ser adequada pelos motivos apresentados no documento, concentrando-se dessa forma, no fato da realização estar dentro do controle de uma organização ou fora dele.

Eficácia

Diversos leitores afirmam que a eficácia do gerenciamento de riscos corporativos deve ser definida em relação aos resultados obtidos, mensurados em termos dos resultados que o processo deve alcançar, em vez de um julgamento subjetivo do fato dos oito componentes estarem ou não presentes e funcionando adequadamente.

O critério de eficácia – a presença e o funcionamento efetivo de cada componente – permanece no documento final. Concluiu-se que o princípio desenvolvido na estrutura de controle interno e transportado para a estrutura de gerenciamento de riscos corporativos é lógico e atende adequadamente às necessidades dos usuários (e inexistem fraquezas significantes), o resultado é que a administração e a diretoria adquirem garantia razoável dos objetivos estipulados. O documento final mantém esse princípio e também ressalta que compatibilizar o risco com o apetite a riscos da organização é um elemento necessário do gerenciamento de riscos corporativos bem-sucedido. O conceito de um julgamento subjetivo em relação à presença e ao funcionamento dos oito componentes foi eliminado pelo fato de que o julgamento pode ser objetivo, com base nos princípios dessa estrutura.

Abrange o Controle Interno

A minuta, apresentada ao público, continha uma parte, mas nem todo o texto de “Controle Interno – Estrutura Integrada”, indicando que a totalidade do documento de controle interno havia sido incorporada por referência na estrutura de gerenciamento de riscos corporativos. A referida minuta incluía um apêndice que compara e contrasta as duas estruturas.

Alguns leitores sugerem que o relatório final deve identificar com maior proeminência as partes transportadas do “Controle Interno – Estrutura Integrada”. Outros recomendam incluir a totalidade do “Controle Interno – Estrutura Integrada” como anexo, com uma reconciliação detalhada das diferenças entre os dois documentos, enquanto que outros sugerem que o documento deve descrever em detalhes o modo em que o “Controle Interno – Estrutura Integrada” é ampliado na estrutura do gerenciamento de riscos corporativos. Finalmente, outros leitores sugerem que o documento ressalte e esclareça qual o grupo-alvo pretendido e a finalidade de cada estrutura.

Concluiu-se que a descrição das diferenças entre as estruturas está no nível apropriado. O “Apêndice C” realça as diferenças fundamentais e identifica os conceitos da estrutura de gerenciamento de riscos corporativos que estão diretamente incorporados com base no “Controle Interno – Estrutura Integrada”, os conceitos extraídos da estrutura de controle interno que foram ampliados e os novos conceitos. Não se considerou necessário incluir a estrutura de controle interno como anexo, pelo fato de que se encontra facilmente disponível aos usuários. Além da finalidade e do grupo-alvo pretendido por cada uma das estruturas, já estão descritos em suficiente detalhe.

O Gerenciamento de Riscos Corporativos e o Processo de Gerenciamento

Alguns leitores sugerem que o anexo que compara as atividades de gerenciamento com as atividades de gerenciamento de riscos corporativos propiciam muito poucas informações e, dessa forma, podem gerar confusão entre os leitores. Alguns afirmam que considerar as atividades de gerenciamento como se fossem diferentes das atividades de gerenciamento de riscos corporativos pode reduzir – ao invés de reforçar – a idéia de incorporar o gerenciamento de riscos às atividades de negócios e de gerenciamento.

O anexo da minuta apresentada ao público não foi transportado para o relatório final e, em seu lugar, mensagens relevantes são apresentadas no texto.

Informação e Comunicação

Determinados leitores tecem comentários sobre a importância de um canal fora das linhas normais de comunicação, sugerindo que esse canal seja um elemento necessário no gerenciamento de riscos corporativos.

O relatório final reflete essa opinião, afirmando que, para que o gerenciamento de riscos corporativos possa ser eficaz, a organização deverá manter o referido canal de comunicação.

Funções e Responsabilidades

Alguns leitores sugerem que é preciso maior clareza em relação às diferentes responsabilidades no gerenciamento de riscos corporativos para o conselho, a administração, os empregados da organização e as partes externas interessadas.

O relatório final amplia o debate e esclarece as respectivas funções e responsabilidades dessas partes.

Outras Considerações

Forma e Apresentação

Alguns leitores comentam sobre o tamanho, o formato e o estilo da minuta de apresentação e expressam inúmeras opiniões novas sobre a maneira pela qual o relatório poderia ser reorganizado e dinamizado.

Concluiu-se que o relatório deveria ser reorganizado e dinamizado para otimizar a sua leitura e clareza e, ainda, reduzir redundâncias. O "Sumário Executivo" da minuta de apresentação foi substituído por um resumo mais breve. O Capítulo 1 da minuta de apresentação, "Importância do Gerenciamento de riscos corporativos," foi suprimido, sendo os conceitos de maior importância incorporados ao capítulo, "Definição", do relatório final. As redundâncias foram reduzidas, as considerações de menor importância eliminadas e o fraseado do relatório foi dinamizado.

Relação entre Gerenciamento de Riscos Corporativos – Estrutura Integrada e Outros Relatórios e Legislação

Alguns leitores afirmam que seria útil discutir as relações entre a estrutura do gerenciamento de riscos corporativos e o Ato Sarbanes-Oxley de 2002, "*The Basel Committee on Banking Supervision's New Basel Capital Accord*", e a legislação de gerenciamento de riscos na Austrália, Canadá, Alemanha, Japão, Reino Unido e outros países. Determinados leitores recomendam que o documento declare expressamente que o "Controle Interno – Estrutura Integrada" continua sendo uma estrutura aceitável para o cumprimento da Seção 404 do Ato Sarbanes-Oxley de 2002, e que a publicação do "Gerenciamento de Riscos Corporativos – Estrutura Integrada" não exija que as Companhias o utilizem para cumprir a Seção 404.

Concluiu-se que a reconciliação do "Gerenciamento de Riscos Corporativos – Estrutura Integrada" está além do alcance do presente projeto. No que diz respeito ao cumprimento dos requisitos da Seção 404 do Ato Sarbanes-Oxley, COSO comunica pelo Prefácio desse relatório, que "Gerenciamento de Riscos Corporativos – Estrutura Integrada" continua implementado e é consultado devidamente como base para informações, em atendimento a determinados requisitos legais, como é o caso do Ato Sarbanes-Oxley de 2002.

Orientação da Aplicação

Alguns leitores recomendam a inclusão de conteúdo específico para o volume de orientação da aplicação. Outros sugerem a inclusão de um ou mais estudos de caso para facilitar a implementação da estrutura por organizações de portes variados. Além disso, sugerem que o documento da “Estrutura” e o da orientação da aplicação apresentem vínculos para o cruzamento de referências.

Concluiu-se que o volume de orientação da aplicação deve conter determinados itens de conteúdo, inclusive ilustrações de como as organizações poderão aplicar conceitos específicos descritos no documento da “Estrutura”. O relatório final contém essas informações, a despeito do fato que se decidiu não ser viável identificar ou desenvolver um estudo de caso para ilustrar a aplicação de todos os conceitos da “Estrutura” e que fazê-lo vai além do alcance desse projeto. Como o enfoque mais nítido do conteúdo desse volume, decidiu-se que o título “Técnicas de Aplicação” seria mais apropriado, após ter sido submetido às revisões necessárias. Além disso, foram incluídos vínculos referenciais do documento “Técnicas de Aplicação para o da Estrutura”.

F. Glossário

Controles de Aplicativos – procedimentos programados em um aplicativo de software e procedimentos manuais associados que são destinados a assegurar sua completude e exatidão do processamento das informações. Os exemplos incluem verificações computadorizadas da edição de dados de entrada, verificações da seqüência numérica e dos procedimentos manuais para o acompanhamento dos itens relacionados nos relatórios de exceção.

Conformidade – empregado com os "objetivos" e relacionado com o cumprimento de leis e regulamentos aplicáveis.

Componentes – há oito componentes do gerenciamento de riscos corporativos: o ambiente interno da organização, a fixação de objetivos, a identificação de eventos, a avaliação de riscos, a resposta a riscos, as atividades de controle, as informações e as comunicações e o Monitoramento.

Controle – 1. Substantivo que denota um item, por exemplo, a existência de um controle, a política ou o procedimento que faz parte do controle interno. O controle pode existir em qualquer um dos oito componentes. 2. Substantivo que indica um estado ou uma condição, por exemplo, efetuar um controle – o resultado de políticas e procedimentos destinados ao controle; esse resultado poderá ou não ser um controle interno eficaz. 3. Verbo, por exemplo, controlar – regular, estabelecer ou implementar uma política que efetue controle.

Critérios – Um conjunto de normas em relação às quais o gerenciamento de riscos corporativos pode ser mensurado para a determinação de sua eficácia. Os oito componentes do gerenciamento de riscos corporativos, considerados no contexto das suas limitações inerentes, representam critérios para sua eficácia em relação a cada uma das quatro categorias de objetivos.

Deficiência – Condição no gerenciamento de riscos corporativos que merece atenção e que pode representar uma desvantagem percebida, em potencial ou real, ou uma oportunidade de fortalecer o processo de gerenciamento de riscos corporativos, de modo a possibilitar uma maior probabilidade que os objetivos da organização serão alcançados.

Desenho – 1. Propósito. Conforme utilizado na definição, gerenciamento de riscos corporativos tem a finalidade de identificar os eventos em potencial capazes de afetar a empresa e gerenciar o risco de modo a mantê-lo em conformidade com o apetite a riscos da referida organização, possibilitar garantia razoável em relação à realização dos objetivos. 2. Plano; o modo pelo qual um processo deve operar, em comparação ao modo pelo qual efetivamente opera.

Efetivo – Usado quando o gerenciamento de riscos corporativos: concebido e operado.

Processo de Gerenciamento de Riscos Corporativos – Sinônimo de gerenciamento de riscos corporativos aplicado em uma organização.

Entidade – Uma organização de qualquer porte estabelecida para o atendimento de uma determinada finalidade. A entidade poderá ser, por exemplo, uma empresa comercial, uma organização sem fins lucrativos, um órgão do governo ou uma instituição acadêmica. Entre os termos empregados como sinônimos estão "organização e empresa".

Evento – Incidente ou ocorrência, a partir de fontes internas ou externas a uma entidade, capaz de afetar a realização dos objetivos.

Controles Gerais – Políticas e procedimentos que contribuem para assegurar uma operação continuada e adequada dos sistemas de informática. Incluem os controles sobre o gerenciamento da tecnologia de informações, a infra-estrutura da tecnologia da informação, a administração da segurança e aquisição, o desenvolvimento e a manutenção de software. Os controles gerais dão suporte ao funcionamento dos controles de aplicações programados. Outros termos também empregados para descrever os controles gerais são controles gerais de computador ou controles de tecnologia da informação.

Impacto – Resultado ou efeito de um evento. Poderá haver uma série de impactos possíveis associados a um evento. O impacto de um evento pode ser positivo ou negativo em relação aos objetivos correlatos de uma empresa.

Limitações Inerentes – Limitações do gerenciamento de riscos corporativos. Dizem respeito a limitações do julgamento humano; restrições de recursos e a necessidade de se considerarem os controles de custos em relação aos benefícios esperados; a realidade que podem ocorrer falhas; e a possibilidade de neutralização de controles e de conluio pela administração.

Risco Inerente – O risco que se apresenta a uma organização na ausência de qualquer medida gerencial que poderia alterar a probabilidade ou o impacto de um risco.

Integridade – A qualidade ou o estado de possuir princípios morais íntegros; retidão, honestidade e sinceridade; o desejo de fazer aquilo que é certo, professar e viver de acordo com uma série de valores e expectativas.

Controle Interno – Processo efetuado pelo conselho, administração ou qualquer outro funcionário de uma empresa, desenhado para fornecer garantia razoável em relação à realização dos objetivos nas seguintes categorias:

- Eficácia e eficiência das operações.
- Confiabilidade dos relatórios financeiros.
- Conformidade com leis e regulamentos aplicáveis.

Sistema de Controle Interno – Sinônimo de controle interno aplicado a uma organização.

Probabilidade - A possibilidade de ocorrência de um dado evento. Os termos podem adquirir conotações mais específicas como indicar "possibilidade" de que um dado evento ocorrerá em termos qualitativos, como elevada, média e reduzida, ou outras escalas de julgamento; e "probabilidade" indicando uma medida quantitativa, como porcentagem, freqüência de ocorrência ou outra unidade numérica de medida.

Intervenção da Administração – As medidas adotadas pela administração para neutralizar políticas ou procedimentos estipulados com fins legítimos; a intervenção da administração geralmente é necessária para tratar de eventos ou transações não recorrentes e não padronizadas ou eventos que, de outro modo, poderiam ser tratados inadequadamente pelo sistema (contrastar esse termo com Neutralização pela Administração).

Neutralização pela Administração – A neutralização de políticas ou procedimentos estipulados com finalidades escusas. Com a intenção de obter vantagens pessoais ou apresentação indevidamente melhorada das condições financeiras da organização, ou da sua situação quanto ao cumprimento de regulamentações e leis (contrastar esse termo com Intervenção da Administração).

Processo de Gerenciamento – O conjunto de medidas adotadas pela administração para operar uma organização. O gerenciamento de riscos corporativos faz parte do processo de gerenciamento, estando integrado a ele.

Controles Manuais – Controles executados manualmente, não por computador.

Categoria de Objetivos – Uma das quatro categorias de objetivos de uma organização – estratégicos, eficácia e eficiência operacionais, confiabilidade dos relatórios e cumprimento de leis e regulamentos cabíveis. As categorias sobrepõem-se. Assim, um determinado objetivo poderá classificar-se em mais de uma categoria.

Operações – Utilizado com os "objetivos" e relacionado com a eficácia e a eficiência das atividades de uma organização, inclusive das metas de desempenho e de lucro, e salvaguarda dos recursos contra prejuízos.

Oportunidade – A possibilidade que um evento ocorrerá e afetará favoravelmente a realização dos objetivos.

Política – A administração estabelece aquilo que deverá ser feito para efetuar o controle. Uma política serve de base para a definição dos procedimentos e sua implementação.

Procedimento – Uma ação que implementa uma política.

Garantia Razoável – O conceito que o gerenciamento de riscos corporativos, independentemente de seu desenho e sua operação, não é capaz de propiciar uma garantia em relação à realização dos objetivos de uma organização. Isso ocorre em razão das Limitações Inerentes do gerenciamento de riscos corporativos.

Comunicação – Utilizado com os "objetivos" e relacionado com o grau de confiabilidade dos relatórios de uma organização, inclusive o relato interno e externo de informações financeiras e não-financeiras.

Risco Residual – O risco que resta após a administração ter adotado medidas para alterar a probabilidade ou o impacto dos riscos.

Risco – A possibilidade de que um evento ocorra e afete desfavoravelmente a realização dos objetivos.

Apetite a Riscos – A quantidade total de riscos que uma companhia ou outra organização está disposta a aceitar na busca de sua missão (ou visão).

Tolerância a Riscos – A variação aceitável relativa à realização de um objetivo.

Partes Interessadas – Partes que são afetadas pela organização, como os acionistas, as comunidades nas quais a organização opera, os empregados, os clientes e os fornecedores.

Estratégico – Utilizado em conjunto com "objetivo" e relacionado com as metas de nível elevado que se alinham à missão (ou à visão) da organização, propiciando-lhe suporte.

Incerteza – Incapacidade de conhecer antecipadamente a probabilidade exata ou o impacto de eventos futuros.

G. Agradecimentos

O Conselho do COSO, Conselho Consultivo e PricewaterhouseCoopers LLP, reconhecem com gratidão a colaboração dos inúmeros executivos, legisladores, agentes normativos, acadêmicos e outros que dedicaram seu tempo e sua energia participando e contribuindo para os diversos aspectos desse estudo. Reconhecemos, também, a inestimável colaboração das organizações e dos membros do COSO que participaram de pesquisas, seminários e reuniões, oferecendo comentários e feedback durante todo o processo de desenvolvimento dessa estrutura.

Os seguintes sócios da PricewaterhouseCoopers forneceram importantes sugestões à essa estrutura: Dick Anderson, Jeffrey Boyle, Gleen Brady, Michael Bridge, John Bromfield, Gary Chamblee, Nicholas Chipman, John Copley, Michael de Crespigny, Stephen Delvecchio, Scott Dillman, P. Gregory Garrison, Bruno Gasser, Susan Kenney, Brian Kinman, Robert Lamoureux, James La Torre, Mike Maali, Jorge Manoel, Cathy Mckeon, Juan Pujadas, Richard Reynolds, Mark Stephen, Robert Sullivan, Jeffrey Thompson e Shyam Venkat.

As seguintes pessoas também contribuíram com esse estudo: Michael Haubenstock, Diretor de Gerenciamento de riscos corporativos, Capital One Finance Corporation; Adrienne Willich, Gerente de Riscos Operacionais, Capital One Finance Corporation; e Daniel Mudge, Presidente e Responsável por Operações de OpVantage, Richard A. Scott, William G. Shenkir e Paul L Walker da Universidade de Virgínia que conduziram as pesquisas preliminares que conduziram a esse estudo. Agradecemos, também, a Myra Clearly pela orientação editorial.

Nossos especiais agradecimentos a William H. Bishop, III, Presidente do Institute of Internal Auditors, que até o seu falecimento trabalhou incansavelmente para otimizar a função e o status da profissão de auditoria. A participação de William H. Bishop, III, nesse projeto e no projeto da estrutura de controle interno do COSO contribuiu para a melhoria dos relatórios. O colega e amigo sempre será lembrado.