Hoje quero trazer para nossa reflexão um tema fundamental para a consolidação da governança corporativa

Vamos falar sobre gerenciamento de riscos corporativos.

Estava preparando o curso, e me deparei com um slide que uso para explicar, a estrutura aplicada para a gestão de riscos, e me senti motivado em trazer este tema para nossa discussão.

Quem já me acompanha pelas redes sociais, sabe que sempre procuro trazer uma visão simples para temas importantes relacionados com gestão e governança, facilitando o entendimento e sua aplicação nas atividades corporativas.

Simplicidade, atualmente, é vantagem competitiva para a organização, mas entenda que ser simples não quer dizer ser superficial.

Bom, vamos voltar para o nosso tema que é gestão de riscos.

De forma simples, posso dizer que:

"***Gerenciar riscos é uma atividade proativa, de olhar para o futuro, entender os eventos, externos e/ou internos, que podem se materializar e impactar adversamente a capacidade da empresa ou do processo alcançar seus objetivos; avaliá-los quanto a sua magnitude, e trata-los com base nos níveis aceitáveis de riscos definidos pela corporação***."

O objetivo primário da gestão de riscos é permitir que a corporação possa, na busca ao cumprimento de sua missão, conduzir, direcionar e manter suas atividades, ações e decisões, dentro do seu nível aceitável de risco, definido pelo apetite a risco.

O ponto de partida para a gestão de riscos é a correta compreensão dos objetivos, sejam eles, estratégicos, corporativos e/ou operacionais. Se não conhecemos os objetivos de forma clara, fica difícil conhecer os riscos de forma compreensiva.

A não utilização dos objetivos como base para a identificação dos riscos é o erro mais comum que encontro nas corporações, fazendo com que sejam gastos tempo e recursos de forma equivocada e não efetiva.

Lembre-se que o evento de risco impacta diretamente na capacidade de alcançar os objetivos.

Em relação aos objetivos operacionais, aqueles que se relacionam com os diversos processos existentes para a operacionalização das atividades da organização, recomendo a definição dos objetivos inerentes a cada um dos processos, como também dos objetivos relacionados com conformidade legal, objetivos relacionados com os valores morais da organização, e objetivos relacionados com a consistência, integridade, confidencialidade e recuperabilidade dos dados processados.

Quanto melhor for a definição dos objetivos, mais eficaz tende a ser a identificação dos riscos.

Bem, uma vez que já determinamos os objetivos, agora iniciamos o processo de identificação dos eventos, externos e/ou internos que possam impactar a corporação.

Depois, de forma simples, começamos a identificar os riscos que, se materializado, impactará adversamente a capacidade da organização alcançar seus objetivos. Podemos ver o risco como a visão negativa do objetivo, exemplo: Se um dos objetivos inerentes de um processo de compra é comprar somente produtos e/ou serviços necessários para a operacionalização da corporação, o risco, poderá ser, a compra de produtos e/ou serviços não necessários para a operação.

Baseado no entendimento dos objetivos, procure identificar todos os eventos de riscos que se relacionam com ele. Esta é uma atividade realizada por meio de “brainstorm”. Não existe uma forma cartesiana para isto.

Uma vez que todos os riscos percebidos estão relacionados, o próximo passo é conhecer suas causas, isto é, os eventos que possam materializar o risco.

São os fatores de riscos (causas) que avaliamos a magnitude e que tratamos, por isso é importante ser criterioso na identificação deles.

Para ilustrar, vamos voltar no exemplo do processo de compras, por qual razão a corporação poderá comprar produtos e/ou serviços não necessários para a operação? As respostas a esta questão nos permitirão identificar os fatores de riscos. Exemplo: a. Uma requisição de compras errada, b. Falta de planejamento dos estoques, c. Uma fraude, e etc.

Este procedimento deve ser realizado para todos os riscos identificados, sem exceção.

Muito bem, neste ponto, nossa matriz de riscos já conta com três colunas básicas: Coluna dos objetivos, coluna dos riscos relacionados com cada um dos objetivos e coluna dos fatores de riscos relacionados com cada um dos riscos identificados.

O próximo passo é a análise e avaliação dos fatores de riscos por meio da leitura matricial de probabilidade (frequência) e impacto (em diversas dimensões, como financeiro, imagem, market-share e outros).

Neste ponto é importante que a corporação tenha métricas, aprovadas pela alta gestão, para a avaliação da magnitude (probabilidade e impacto) dos fatores de riscos.

Também é importante que a empresa já tenha o apetite a risco definido pela alta gestão. Como sugestão, para facilitar o processo de gerenciamento de riscos, oriente a alta gestão para definir o apetite a risco com base no mapa de calor resultante das métricas, indicando o quadrante que deve ser considerado como o nível aceitável de risco.

Gosto de utilizar métricas com cinco níveis de probabilidade e cinco níveis de impacto, de forma que o mapa de calor tenha quadrantes de 01 a 25. Neste caso, o apetite a risco pode ser definido como sendo um dos quadrantes existentes, por exemplo a alta gestão pode direcionar que seu apetite a riscos seja o quadrante seis, de forma que tudo que estiver acima precisará ser tratado.

Um dos problemas que me deparo, nesta etapa de avaliação, é em relação à utilização das métricas complexas, com a inclusão de pesos, média ponderada e outros cálculos que somente trazem complexidade e morosidade para o processo.

Observe que, mais importante do que a acuracidade da medição do fator de risco, é ação que a gestão toma para tratamento dele. Não importa se o risco é 15,234 ou 15, o que realmente importa é a ação que a gestão toma para a mitigação do fator de risco.

O cálculo é simples: probabilidade x impacto = Risco bruto

Outro ponto importante nesta etapa da avaliação, é na definição do impacto, isto é, se o evento se materializar, qual o impacto que ele trará para a organização. Algumas corporações procuram avaliar o impacto por meio de média ponderada entre as diversas dimensões. A sugestão é trabalhar com a dimensão que recebe o impacto primário, e não com média ponderada do impacto nas diversas dimensões, pois, observe que não é assim que acontece na realidade. Exemplo: se o evento se materializa e impacta a imagem, não necessariamente ele impactará, simultaneamente, as outras dimensões medidas, de forma que o melhor é se concentrar no tratamento do efeito na imagem, procurando que ela não afete de forma secundaria as outras dimensões.

Muito bem, agora que conhecemos a magnitude bruta (risco bruto) para todos os fatores de riscos, sejam eles inerentes, de compliance, fraude, ou de TI, a próxima etapa é comparar a magnitude obtida com o apetite a riscos, e com base nisto, determinar qual o melhor tratamento para alinhar o risco bruto com o apetite a risco determinado pela organização.

Mantenha em mente que o objetivo primário do gerenciamento de riscos é permitir que a corporação atue dentro de seu nível aceitável de risco, formalizado por meio da definição do apetite a risco.

O tratamento do fator de risco pode ser: Aceitar, Compartilhar, Evitar e mitigar.

Podemos aceitar o risco, quando o risco bruto já esteja alinhado ou abaixo do apetite a risco, entretanto aceitar o risco, não significa não fazer nada, mas sim, monitorar os fatores de risco, pois hoje ele está baixo, amanhã poderá mudar e com isto mudar nosso tratamento. Outro ponto importante é em relação a quem pode aceitar o risco, e minha sugestão é que seja pelos gestores estatutários, uma vez que legalmente são eles que correm o risco pela empresa, inclusive com seus bens pessoais.

Compartilhar o risco é um processo onde uma outra corporação, seja ela uma instituição financeira ou uma seguradora, aceite correr parte do risco pela empresa. Exemplo: Apólices de seguros, ou realização de hedge cambial. Observe que está é uma resposta no impacto e não na probabilidade.

Outra forma de tratamento para os fatores de riscos é evitar o risco. É uma das respostas mais difíceis de se trabalhar, pois para evita os riscos, a organização não pode mais estar exposta ao risco, o que significa, na grande maioria das vezes, tomadas de decisões estratégicas, como a saída da empresa de um mercado, ou o fechamento de uma unidade, ou não realização de uma operação

e etc.

Por último temos a possibilidade de mitigação do fator de risco, o que operacionalmente falando, requer a implementação de um controle interno para a mitigação da probabilidade do evento de risco se materializar. Somente lembrando que controle interno são:

“***Ações, formalizadas em políticas e procedimentos, que visão a mitigação da probabilidade de materialização do evento de risco. São ações de revisão, conferência, certificação, validação, autorização, aprovação e etc.***”

Dependendo da materialidade e natureza do risco, além da resposta na probabilidade, será necessário a elaboração de um plano de contingência, o qual visa, minimizar o efeito do impacto, quando da materialização do evento de risco.

Uma vez que as respostas foram determinadas e implementadas, o próximo passo é calcular o risco residual, que é o efeito remanescente após a ação de tratamento, e certificar que esteja alinhado com o apetite a risco definido pela corporação.

Lembre-se que a simplicidade, atualmente, é vantagem competitiva! Traga simplicidade para a operação, e não superficialidade!

Seja Feliz!

20.07.2022