Contar com um bom e estruturado processo de gerenciamento de riscos é fundamental para a consolidação de uma gestão pautada em boas práticas de governança. Sabemos que a gestão de riscos aumenta a capacidade da organização em atingir seus objetivos estratégicos que se estiverem alinhados a sua missão, possibilitará criar valor às partes relacionadas.

Atualmente uma grande gama de normas, regulamentos e leis estabelecem a obrigatoriedade do gerenciamento de riscos pelas organizações, como exemplo: Instrução Normativa Conjunta MP/CGU 01, Circular Susep 521, Lei 13.303, sem falar as normas do Banco Central, CVM e outras, o que está motivando uma onda de implementação nas organizações do setor privado e público.

Antes de mais nada, precisamos observar que gerenciar riscos não é algo a mais que o gestor deve fazer, mas simplesmente é o que ele tem que fazer para gerenciar qualquer processo ou atividade por qual é responsável.

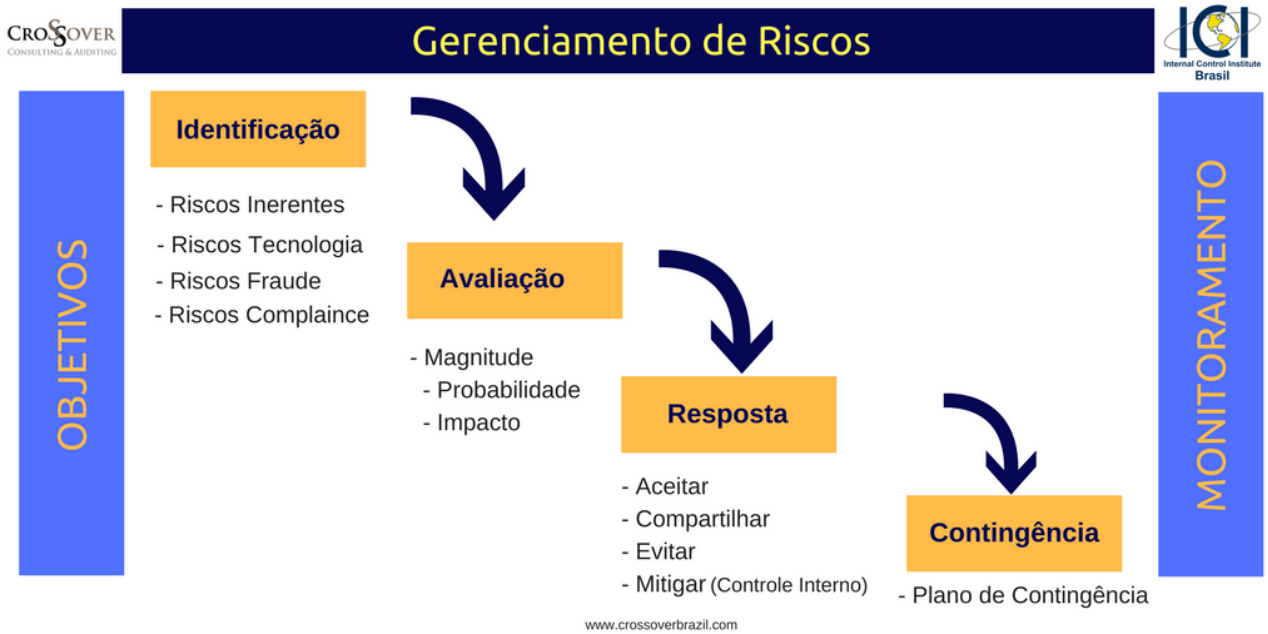
Uma gestão baseada em riscos deve trabalhar com a seguinte visão:

OBJETIVO – RISCOS – TRATAMENTO DOS RISCOS

O risco está intimamente relacionado com os objetivos, isto é, se não tivermos ou conhecermos os objetivos, não temos como identificar os riscos inerentes, aqueles que se relacionam diretamente com o risco.

De uma forma simples, risco é todo o evento que impacta negativamente a capacidade de alcançarmos o objetivo. Então uma vez que já temos a consciência de que o risco existe precisamos de um processo para poder identifica-lo e trata-lo, de forma a aumentar as chances da organização de alcançar os objetivos pré-estabelecidos.

Conceitualmente, a gestão de riscos é o processo de: Identificação dos riscos, avaliações de sua magnitude, tratamento dos riscos e se necessário, dependendo da magnitude do risco, criar um plano de contingência.



Vejamos cada uma destas atividades para avaliação dos riscos de um processo operacional:

1. Identificação dos Riscos

Nesta etapa precisamos antes de mais nada definir os objetivos do processo que será avaliado. Nesta etapa quanto mais detalhado for definido o objetivo, melhor será para iniciar a identificação dos riscos inerentes. O risco inerente é a negativa do objetivo, exemplo: Se o objetivo do processo for comprar apenas serviços e produtos necessários para a operação, os riscos inerentes serão: Não comprar e Comprar o que não for necessário. A forma mais utilizada para identificação dos riscos é o “Brainstorm”, o qual poderá ser apoiado por algumas outras ferramentas, como: Ishikawa, BowTie e etc.

Nesta etapa é necessário identificar os riscos de conformidade legal, da aplicação da tecnologia da informação e também de fraude. O processo é o mesmo, com pequenas diferenças na definição dos objetivos. Além dos riscos é importante identificar as causas dos riscos, também conhecido como fator de riscos.

A formalização desta etapa pode ser em uma planilha simples, onde na primeira coluna são definidos os objetivos, na segunda coluna são identificados os riscos para cada objetivo e a terceira coluna são identificados os fatores de riscos para cada um dos riscos identificados.

2. Avaliação da Magnitude

O risco pode ser medido e isto é feito de forma matricial através da leitura da probabilidade e impacto. Neste ponto é fundamental que a empresa tenha uma régua para fazer esta medição de forma objetiva, mesmo sabendo que existe uma grande subjetividade neste processo. O desafio aqui é ser o mais simples dentro da complexidade da operação. De nada adianta ter modelos matemáticos sofisticados se no final o gestor ou especialista terá que ter uma posição subjetiva. Para a formalização desta medição, sugerimos que sejam acrescidas três colunas na planilha utilizada para a formalização dos riscos acima, sendo: uma para a probabilidade, outra para o impacto e uma para a magnitude (resultado da probabilidade e impacto)

3. Tratamento dos riscos

O risco poderá ser tratado somente após ter sua magnitude conhecida, pois para definir a resposta, o apetite e a tolerância ao risco deverão ser considerados. Existem quatro formas básicas de respostas: Aceitar o risco, compartilhar o risco, evitar o risco e mitigar o risco. Quando falamos em mitigar o risco operacional, estamos falando em definir um controle interno para dar resposta a probabilidade ou ao impacto, muito mais na probabilidade. A ideia com o controle interno é trazer o risco bruto ao risco residual para o nível de apetite a risco da organização. Aqui sugerimos a elaboração de uma matriz de controle onde todos os controles internos identificados no fluxo do processo sejam identificados quanto ao seu objetivo, responsável, evidencia, tipo, natureza, periodicidade, etc.

4. Contingência

Dependendo da magnitude do risco será necessário a criação de um plano de contingência. Sabemos que um controle interno não é absoluto, ele pode falhar, e por isso é necessário ter um plano para reduzir o impacto do evento, resultado da falha do controle. Quando a resposta for diretamente no impacto, em casos de fatores externos, a mitigação não será um controle, mas sim, um plano contingencial para redução do impacto se o evento se materializar.

Como podem observar o gerenciamento de riscos não é complexo. Em termos formais é necessário que a organização seja “fatiada” em ciclos de negócio e os mesmos em processos operacionais. Para cada processo deve existir um fluxograma, a matriz de riscos, a matriz de controles internos.

O outro passo é executar o alinhamento matriz de riscos com a matriz de controle, para que se

possa conhecer: o controle que está associado a riscos, controle que não tem risco associado e riscos que não tem controle associados.

Os controles que estão associados a riscos serão avaliados quanto a seu desenho e quanto a sua efetividade. Para os controles sem riscos associados será avaliado a razão de sua existência e a possibilidade de sua eliminação. Para os riscos sem controles será avaliado a razão e se é necessário a implantação de um controle ou não.

Para o processo de gerenciamento de riscos não é necessário seguir uma melhor prática, contudo é recomendável. Você pode definir uma melhor prática, seja ela a estrutura do COSO ICF, COSO ERM ou ISO 31.000, e comparar com o processo de sua organização, conhecendo os “gaps” de aderência, fazendo os ajustes necessários para a redução destes “gaps”.

O maior desafio, não é o processo de gerenciamento de riscos em si, é fazer que ele seja parte da cultura da organização, criando consciência para riscos no ambiente interno.

E para finalizar, não implemente um processo de gerenciamento de riscos sem elaborar um projeto onde sejam definidos os fatores de sucesso.

Façam da forma mais simples possível dentro da complexidade da organização, pois complexidade custa caro e nem sempre é efetiva!

Seja Feliz!

(09.05.2018)

CROSSOVER
CONSULTING & AUDITING