No último artigo abordamos as mudanças mais significativas da nova estrutura de controle interno publicada pelo COSO. Neste artigo quero tratar especificamente do componente denominado como avaliação de risco (risk Assessment). Tenho observado nos cursos e nos projetos de consultoria que ainda pairam muitas dúvidas sobre este tema, principalmente no atendimento deste quesito no processo de implantação de um sistema de controle interno aderente a esta melhor prática.

Antes de seguir em frente é imperativo relembrar o conceito de risco definido pelo *Committee of Sponsoring Organizations of the Treadway Commission* – COSO, vejamos:

“Risco é a possibilidade de que um evento ocorra e impacte negativamente a condição da empresa de atingir objetivos previamente estabelecidos.”

Fica claro, através da definição acima, a necessidade de conhecermos os objetivos operacionais, para que possamos pensar em riscos, pois, se não for desta forma, o processo de avaliação de riscos poderá não ser eficaz. A estrutura COSO ICF solicita que trabalhemos três objetivos básicos, são eles:

- **Operacional** – Responsável pela eficiência, eficácia e economia dos processos operacionais,
- **“Reporting”** – Responsável pela exatidão e consistência dos registros dos dados e informações originadas e/ou processadas através dos processos operacionais,
- **Conformidade** – Este objetivo é responsável pela empresa estar em conformidade com Leis, normas e regulamentos através dos processos operacionais.

Importante mencionar que um processo operacional somente tem razão de existir se ele tiver uma conexão clara com os objetivos estratégicos da organização. Assim, é mandatório identificar, de maneira detalhada, os objetivos de cada um dos processos operacionais existentes na empresa.

Como já sabemos, esta nova estrutura COSO conta com 17 princípios relacionados com os cinco componentes. Para este componente, existem quatro princípios definidos, são eles:

1. A organização especifica os objetivos com clareza suficiente, de modo a permitir a identificação e avaliação dos riscos associados aos objetivos,
2. A organização identifica os riscos à realização de seus objetivos por toda a entidade, e analisa os riscos como uma base para determinar de que forma os riscos devem ser gerenciados,
3. A organização considera o potencial de fraudes na avaliação dos riscos à realização dos objetivos,
4. A organização identifica e avalia as mudanças que poderiam afetar de forma significativa o

sistema de controles interno.

De uma maneira simples, o processo de avaliação de riscos é composto por três etapas distintas: a - Identificação dos riscos, b - avaliação da magnitude do risco através da leitura matricial de probabilidade e impacto, c - identificação da resposta ao risco e implementação da atividade de controle. Importante frisar, que na avaliação de riscos operacionais, quando falamos de mitigação dos riscos, estamos falando da inclusão de uma atividade de controle interno como resposta ao risco, mitigando a probabilidade de ocorrência, e/ou minimizando o impacto.

Como normalmente não é possível avaliar todos os processos operacionais da organização em um curto espaço de tempo, será necessária a definição de um plano de trabalho, e minha sugestão é que você elabore uma lista de processos baseada na magnitude dos riscos envolvidos. Para isto os passos sugeridos são:

- Elabore um mapa de riscos para identificar os processos operacionais com maior materialidade e risco de impactar a condição da empresa não atingir os seus objetivos estratégicos,
- Determine o alinhamento do processo com os objetivos estratégicos,
- Elabore uma lista de processos operacionais com maior risco para os com menor risco, de forma que você possa avaliar primeiro os processos com maior risco. Isto não quer dizer que os processos de baixo risco não serão avaliados, é simplesmente uma forma mais eficiente de direcionarmos os recursos da área de controles internos primeiramente para os processos com maior risco.

Muito bem, agora que conhecemos os conceitos importantes, de forma prática, indico os seguintes procedimentos para o atendimento dos princípios do COSO para este componente de avaliação de riscos, são eles:

- Identifique os objetivos do processo operacional sob avaliação. Importante mencionar que quanto mais analítico for a identificação dos objetivos, mais fácil será a identificação dos riscos inerentes associados aos objetivos. Lembre-se: procure categorizar os objetivos em eficiência e eficácia, confiabilidade das informações e conformidade com normas e procedimentos. Para as empresas operando em setores altamente regulamentado o objetivo de conformidade é de extrema relevância;
- Com base nos objetivos identificados, elabore um inventário de riscos inerentes, isto é, riscos associados com cada um dos objetivos. Poderá ser relevante, nesta etapa, a identificação dos fatores de riscos, pois, muitas vezes as respostas ao risco são mais apropriadas para o fator de risco, do que para o risco propriamente dito;
- Baseado nas características do processo avaliado é necessário identificar as ameaças de ocorrência de fraude, identificando, inclusive, as vulnerabilidades do processo, isto é, se acontecer uma fraude onde, no processo, ela ocorrerá;
- Identifique os riscos de TI que possam impactar o processo, principalmente quanto ao: acesso, processamento, segurança e rastreabilidade dos dados e informações;
- Elabore uma matriz de risco para o processo, avaliando a probabilidade de ocorrência e ocorrendo, o seu impacto. A legenda/tabela utilizada nesta avaliação deve ser padrão para a organização, de maneira que exista comparabilidade e amplo entendimento da avaliação;
- O próximo passo é o alinhamento das atividades de controles, identificadas no fluxograma do processo, com os riscos identificados acima. Neste ponto, você poderá encontrar riscos que não tem nenhum controle associado, controle que não tem nenhum risco associado, ou então, controles associados a um ou mais riscos, e vice-versa;
- Para os riscos sem nenhum controle associado é importante avaliar a possibilidade de adoção de um novo controle, lembrando que controle interno tem custo;
- Para controles internos sem nenhum risco associado, é necessário avaliar a possibilidade de eliminação do mesmo;
- Para controles associados aos riscos é necessário avaliar e testar sua efetividade quanto á

resposta ao risco.

A avaliação de riscos deve ser um processo dinâmico, pois, os riscos inerentes ao processo são influenciados pelo ambiente de negócios e por fatores externos e internos, fatores este, que podem ser desde uma alteração na legislação até a implementação de um novo sistema de processamento de dados.

Para finalizar, gostaria de frisar que o gerenciamento de riscos e do sistema de controles internos é uma responsabilidade da alta administração e também do gestor responsável pelo processo operacional. O especialista em controles internos é o apoio especializado para que os gestores desempenhem suas responsabilidades de governança com eficiência e eficácia.