ABNT NBR ISO 31000:2009 - Gestão de Riscos – Princípios e Diretrizes

Todas as organizações gerenciam risco em algum grau, e a norma ISO 31000 traz princípios para a gestão eficaz de riscos.

Para a ISO 31000, risco é "o efeito da incerteza nos objetivos", e a incerteza é "o resultado da falta de conhecimento". A falta de conhecimento é, portanto a fonte dos riscos. Convém frisar, no entanto, que risco e incerteza não são sinônimos. Risco normalmente é caracterizado por um valor, em geral a produtória de probabilidade de ocorrência e severidade do efeito, e incerteza é caracterizada por uma faixa de valores, dentro da qual, para certa probabilidade, encontra-se o valor verdadeiro da grandeza mensurada.

A gestão de riscos é, conforme a norma, "o conjunto de atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos". Este processo envolve:

- mandato e comprometimento: A Alta Direção deve liderar e sustentar o processo.
- concepção da estrutura para gerenciar riscos: compreender o contexto interno e externo da organização (incluindo histórico de ocorrências, mudanças ocorridas ou previstas, etc.), estabelecer uma política de gestão de riscos, definir responsabilidades e autoridades, integrar a gestão de risco nos processos organizacionais, alocar recursos apropriados, estabelecer mecanismos de comunicação e relato internos e externos.
- implementação da gestão de riscos: estabelecer e cumprir um plano de gestão de riscos, baseado em uma estratégia e política de gestão de riscos, atendendo a requisitos legais e regulatórios, informando, treinando e comunicando os envolvidos e tomando decisões apropriadas.
- monitoramento e análise crítica de riscos: uso de indicadores de desempenho, análise periódica e relato e tomada de decisões sobre risco e a própria estrutura.
- melhoria contínua da estrutura: por meio do aprendizado e da melhoria na cultura para gestão de riscos.

A comunicação e consulta às partes interessadas deve ocorrer durante todas as fases da gestão de risco, para obter diferentes pontos de vista e obter apoio.

O contexto externo é o ambiente onde a organização busca atingir seus objetivos (mercado, região, cultura etc.) e o contexto interno é seu ambiente interno (cultura da organização, sistemas de informação, procedimentos, recursos etc.). Devem ser estabelecidos recursos apropriados para o contexto da gestão de risco. Devem ser estabelecidos critérios para determinar a significância do risco.

Podem ser utilizadas diversas técnicas para avaliação de risco (ex.: HAZOP, FMEA, matriz probabilidade X gravidade etc.). Estas ferramentas podem auxiliar na identificação das fontes de riscos, análise e avaliação destes riscos e tratamento dos riscos significativos. Entre as opções para tratamento de riscos estão: eliminar o risco, mitigar o risco ou aceitar o risco. O plano para tratamento dos riscos deve incluir prazos e responsáveis. Este plano deve ser acompanhado e registros devem ser mantidos.

A Lato Qualitas pode auxiliar sua empresa a gerir melhor seus riscos.

Publicado Jul/15 – Nasario de S.F.Duarte Jr.