Glossário

Extraído do manual:

Auditoria Baseada em Riscos -
Como implementar a ABR nas organizações: uma abordagem inovadora

Análise de Riscos: uso sistemático das informações disponíveis para determinar a probabilidade de que ocorram eventos especificados e a magnitude de suas conseqüências, isto é, seu impacto.

Apetite por Riscos: nível de risco considerado aceitável pelo conselho ou direção, que pode ser estabelecido em relação à organização como um todo, para grupos diferentes de riscos ou em termos de riscos individuais.

Arcabouço *(Framework)* de Gestão de Riscos: totalidade de estruturas, metodologia, procedimentos e definições que uma organização decidiu utilizar para implementar seus processos de gestão de riscos.

Auditoria Baseada em Riscos: metodologia que fornece garantia de que o arcabouço de gestão de riscos está operando conforme requerido pelo conselho.

Avaliação de Riscos: processo utilizado para determinar as prioridades da gestão de riscos através da comparação do nível de risco com padrões, níveis-alvo de risco ou outros critérios pré-determinados.

Cadastro de Riscos: lista completa, identificada pela direção, dos riscos que ameaçam os objetivos da organização.

Conselho: grupo diretivo de uma organização, como o conselho de administração, conselho de diretores, chefe de uma agência ou órgão legislativo, conselho de governantes ou curadores de uma organização sem fins lucrativos.

Controle: qualquer ação tomada pela direção, pelo conselho e por outras partes para gerenciar os riscos e aumentar a probabilidade de que os objetivos e metas estabelecidos sejam atingidos. A direção planeja, organiza e dirige o desempenho das ações necessárias para manter os riscos em um nível aceitável, ou para aumentar a probabilidade do resultado desejado.

Corporação: qualquer organização estabelecida para atingir um conjunto de objetivos.

Diretor: membro de um conselho de comando, como o diretor da empresa, curador, conselheiro ou governante.

Facilitação: trabalho com um grupo (ou indivíduo) para tornar mais fácil para o grupo (ou indivíduo) atingir os objetivos que o grupo tenha estabelecido para a reunião ou atividade. Isso envolve ouvir, observar, questionar e apoiar o grupo e seus membros. Não envolve realizar o trabalho nem tomar decisões.

Garantia: apresentação de uma opinião ou conclusão em relação à credibilidade das informações divulgadas e ao processo que fornece tais informações, ou em relação à confiabilidade dos processos de acordo com sua conformidade com certos critérios. O receptor da opinião pode ficar seguro ou não, dependendo de outras influências por ele sofridas.

Gestão Corporativa de Riscos (EWRM – *Enterprise-wide Risk Management*): processo estruturado, consistente e contínuo em toda a organização, para identificar, avaliar, estabelecer respostas e relatar oportunidades e ameaças que afetam a consecução de seus objetivos.

Identificação de Riscos: processo para determinar quais eventos podem ocorrer e afetar os objetivos da organização, e quais são suas causas-raízes.

Manejo de Riscos: implementação das respostas a riscos, que reduzem suas ameaças para abaixo do nível do apetite por riscos. Quando isso não for possível, deve-se relatar o risco ao conselho.

Maturidade de Riscos: grau de adoção e aplicação, por parte da direção, de uma abordagem de gestão de riscos robusta, conforme planejada, em toda a organização, a fim de identificar, avaliar, decidir sobre respostas e relatar oportunidades e ameaças que afetam a consecução dos objetivos da organização.

Monitoramento: processos que relatam à direção, em intervalos apropriados, o sucesso, ou não, das respostas a riscos.

Plano de Auditorias Periódicas: lista de auditorias a serem conduzidas em um período de tempo especificado.

Pontuação de Controle: diferença entre a pontuação do risco inerente e a pontuação do risco residual em um sistema quantitativo. Quanto maior for o valor, maior será a importância da gama de respostas que criarão a diferença. Também conhecida como ‘pontuação de resposta’.

Processo de Avaliação de Riscos: processo completo de identificação, análise e avaliação de riscos.

Processos de Gestão de Riscos: processos para identificar, analisar, avaliar, manejar e controlar eventos ou situações potenciais, a fim de fornecer garantia adequada em relação à consecução dos objetivos da organização.

Respostas a Riscos: meios através dos quais uma organização decide gerenciar cada risco. As principais categorias são: eliminar a atividade geradora do risco; tolerar o risco; transferi-lo para outra organização; ou tratá-lo, reduzindo seu impacto ou probabilidade. Controles internos são uma forma de tratar um risco.

Risco: possibilidade de ocorrência de um evento que terá um impacto na consecução dos objetivos. O risco é mensurado em termos de conseqüência e probabilidade.

Risco Inerente (ou Bruto): situação de um risco (mensurado em termos de impacto e probabilidade) sem levar em consideração qualquer resposta ao risco que a organização possa já ter adotado.

Risco Residual (ou Líquido): situação de um risco (mensurado em termos de impacto e probabilidade) após levar em consideração qualquer resposta de gestão de riscos que a organização possa já ter adotado.

Serviços de Consultoria: atividades de aconselhamento e outras relacionadas a serviços a clientes, cuja natureza e escopo são acordados com o cliente e cuja finalidade é agregar valor e melhorar os processos da organização de governança, gestão de riscos e os de controle, sem que o auditor interno assuma responsabilidades gerenciais. São exemplos: pareceres, conselhos, facilitação e treinamento.

Serviços de Garantia: exame objetivo de evidências com o propósito de fornecer à organização uma avaliação independente dos processos de gestão de riscos, processos de controle ou processos de governança. São exemplos: exames financeiros, de desempenho, de conformidade legal, de segurança e *due diligence*.

Universo de Auditorias: lista de auditorias que mostra os processos por elas cobertos e a importância ou prioridade desses processos.