QSP
CENTRO DA QUALIDADE, SEGURANÇA E PRODUTIVIDADE PARA O BRASIL E AMÉRICA LATINA

QSP
Informe Reservado
Nº 70 – Junho/2007

Implemente a Auditoria Baseada em Riscos em sua organização!

Francesco De Cicco
Diretor-Executivo do QSP
Coordenador do NGR

Introdução

O foco do trabalho dos auditores internos mudou tremendamente na última década. Houve uma transição da auditoria baseada em sistemas para a auditoria baseada em processos, e a ênfase atual é na Auditoria Baseada em Riscos (ABR).

A ABR é um termo muito usado e muito mal compreendido. Este *paper* visa a apresentar a posição do QSP/NGR - Núcleo de Gestão de Riscos em relação à ABR e oferecer algumas diretrizes gerais sobre como abordá-la e praticá-la.

O presente *paper* foi pautado no conteúdo do Manual *Como implementar a Auditoria Baseada em Riscos nas organizações: uma abordagem inovadora*, lançado recentemente pelo QSP.

Contexto

A definição atual de auditoria interna adotada pelo IIA – *The Institute of Internal Auditors*, do Reino Unido, e subscrita pelo QSP/NGR, é:

"Atividade independente de garantia e consultoria, designada para agregar valor e melhorar as operações de uma organização. Auxilia a organização a atingir seus objetivos aplicando uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de gestão de riscos, controles e governança."

Os auditores internos devem adotar uma abordagem baseada em riscos compatível com a abordagem adotada por sua organização. Há muitos enfoques que poderiam ser utilizados, dependendo de quanto a auditoria interna é capaz de se apoiar nos processos de gestão de riscos da organização. Isso possibilita ao auditor evitar a duplicação dos processos já realizados pela direção e lhe permite questionar os processos e as conclusões da direção sobre os riscos da companhia.

Pode ser que os auditores internos digam que sempre concentraram seus esforços nas áreas de maiores riscos da organização. Contudo, a experiência mostra que essa abordagem tem sido direcionada pela avaliação de riscos efetuada pela própria auditoria interna. A principal diferença é que o foco da ABR é entender e analisar a avaliação de riscos efetuada pela direção e basear os esforços de auditoria em torno dessa avaliação.

Quais os objetivos da Auditoria Baseada em Riscos?

O principal objetivo da ABR é fornecer garantia independente para o conselho de administração (ou para a alta direção) da organização de que:

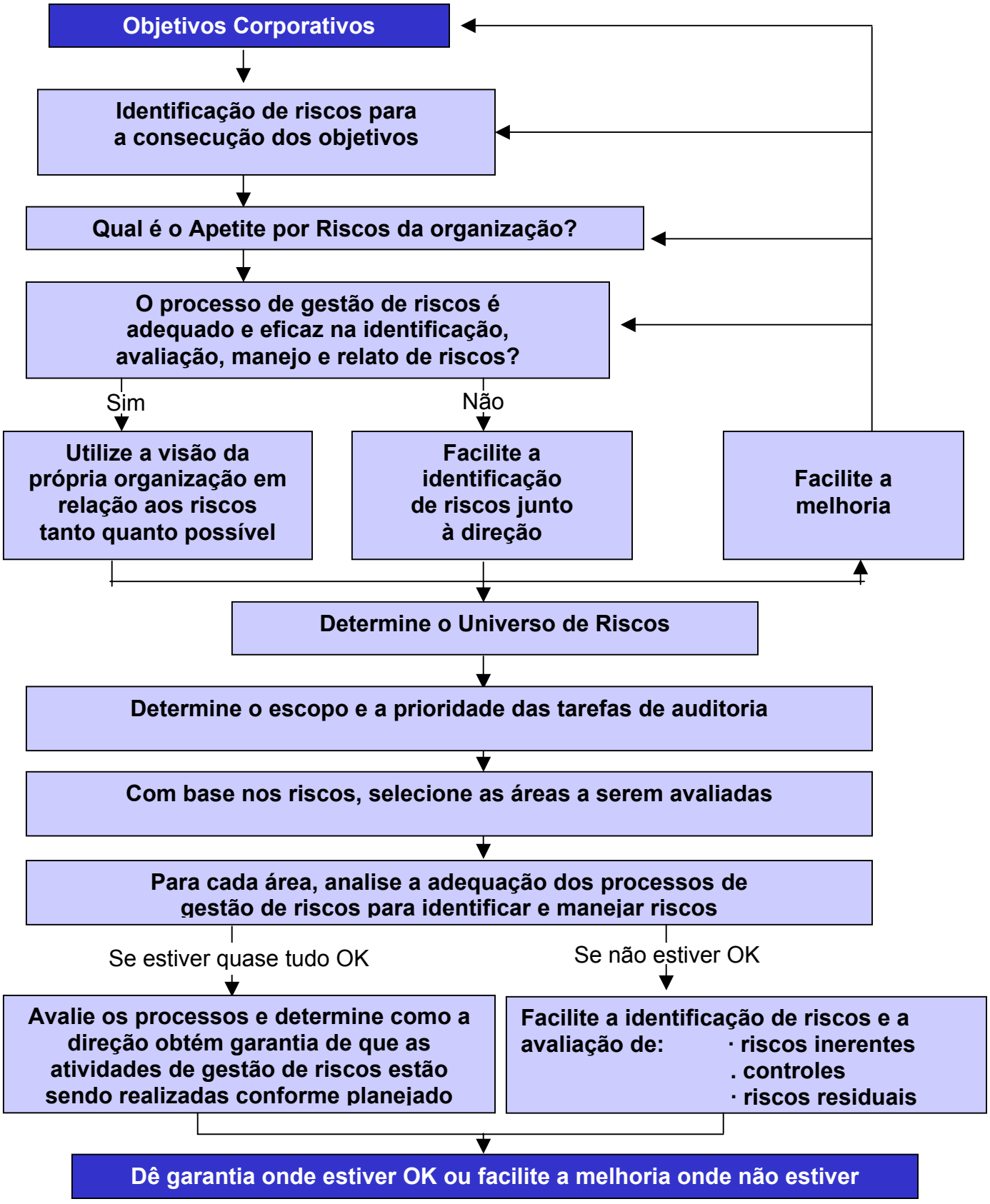
- os processos de gestão de riscos colocados em prática na empresa (abrangendo todos os níveis da companhia) estão operando conforme planejado;
- tais processos de gestão de riscos têm um arcabouço sólido;
- as respostas que a direção tem dado aos riscos são adequadas e eficazes na redução desses riscos a um nível aceitável para o conselho;
- está em vigor uma estrutura sólida de controles para mitigar suficientemente os riscos que a direção deseja tratar.

A ABR começa com os objetivos do negócio e se concentra nos riscos que foram identificados pela direção e que podem comprometer a consecução desses objetivos.

O papel da auditoria interna é avaliar até que ponto é adotada e aplicada uma abordagem robusta de gestão de riscos pela direção em toda a organização, conforme planejado, para reduzir riscos a um nível aceitável (o chamado Apetite por Riscos).

Embora a principal contribuição da auditoria interna seja fornecer garantia sobre o tratamento de riscos efetuado na organização (mediante processos de governança e controles), ela também pode aconselhar quanto a outros aspectos de resposta aos riscos, como as decisões de terminar, transferir ou tolerar riscos.

A abordagem da Auditoria Baseada em Riscos é descrita a seguir de forma esquemática:


Objetivos Corporativos
Identificação de riscos para a consecução dos objetivos
Qual é o Apetite por Riscos da organização?
O processo de gestão de riscos é adequado e eficaz na identificação, avaliação, manejo e relato de riscos?
Sim
Não
Utilize a visão da própria organização em relação aos riscos tanto quanto possível
Facilite a identificação de riscos junto à direção
Facilite a melhoria
Determine o Universo de Riscos
Determine o escopo e a prioridade das tarefas de auditoria
Com base nos riscos, selecione as áreas a serem avaliadas
Para cada área, analise a adequação dos processos de gestão de riscos para identificar e manejar riscos
Se estiver quase tudo OK
Se não estiver OK
Avalie os processos e determine como a direção obtém garantia de que as atividades de gestão de riscos estão sendo realizadas conforme planejado
Facilite a identificação de riscos e a avaliação de: · riscos inerentes . controles · riscos residuais
Dê garantia onde estiver OK ou facilite a melhoria onde não estiver

A prática da Auditoria Baseada em Riscos

Pontos importantes:

- O escopo da ABR inclui riscos estratégicos e riscos do negócio.

- O ponto de partida é determinar se a organização estabeleceu objetivos apropriados, e então determinar se a empresa tem ou não um processo adequado para identificar, avaliar e manejar os riscos que causam impacto nesses objetivos.

- Num ambiente maduro de gestão de riscos, o foco do trabalho de auditoria pode ser:
    - auditar a infra-estrutura de gestão de riscos como, por exemplo, recursos, documentação, métodos e relatórios;
    - auditar o sistema de controles de toda a organização e de cada área ou departamento;
    - realizar auditorias individuais que sejam predominantemente sobre riscos específicos. Caso vários riscos sejam controlados através de um sistema ou processo comum, talvez seja apropriado realizar uma auditoria combinada desse sistema ou processo.

- Em ambientes de gestão de riscos menos maduros, caso as tarefas das auditorias individuais focalizem predominantemente todo um sistema, processo ou unidade de negócio, a auditoria interna deve analisar criticamente os objetivos do negócio e os processos de gestão de riscos dentro de cada uma dessas partes auditáveis.

- Quando os processos de gestão de riscos forem adequados e enraizados, a auditoria interna, quando possível, se apóia na própria visão da organização com relação aos riscos, a fim de determinar o trabalho de auditoria que ela necessita conduzir.

- Quando não puder se basear nos processos de gestão de riscos, a auditoria interna deve realizar sua própria avaliação de riscos (em conjunto com a direção), para determinar o nível preciso do trabalho necessário, e então focalizar a forma como a direção se assegura de que as atividades de gestão de riscos estão sendo praticadas conforme o planejado.

- O resultado final de cada tarefa de auditoria individual deve ser assegurar que os riscos estão sendo gerenciados dentro de um nível aceitável (conforme definido no Apetite por Riscos da organização), ou facilitar e/ou definir melhorias conforme necessário.

Processo contínuo de gestão de riscos

É óbvio, mas é importante enfatizar, que nem todas as organizações estão no mesmo estágio de implementação da gestão de riscos. O diagrama a seguir estabelece uma série de graus de maturidade da gestão de riscos e a abordagem da auditoria interna que pode ser adotada em cada estágio.

Grau de Maturidade da Gestão de Riscos	Características Principais	Abordagem da Auditoria Interna
Ingênuo	Nenhuma abordagem formal desenvolvida para a gestão de riscos.	Promove a gestão de riscos e se baseia na avaliação de riscos da própria auditoria.
Consciente	Abordagem para a gestão de riscos dispersa em "silos".	Promove a abordagem corporativa de gestão de riscos e se baseia na avaliação de riscos da própria auditoria.
Definido	Estratégia e políticas implementadas e comunicadas. Apetite por Riscos definido.	Facilita a gestão de riscos/se relaciona com a gestão de riscos e usa a avaliação dos riscos pela direção quando apropriado.
Gerenciado	Abordagem corporativa para a gestão de riscos desenvolvida e comunicada.	Audita os processos de gestão de riscos e utiliza a avaliação dos riscos pela direção conforme apropriado.
Habilitado	Gestão de riscos e controles internos totalmente incorporados às operações.	Audita os processos de gestão de riscos e utiliza a avaliação dos riscos pela direção conforme apropriado.

Cada organização deve determinar como ela deseja implementar a gestão de riscos. Isso ajudará a determinar seu Apetite por Riscos e o nível de "Maturidade de Riscos". Por exemplo, nem todas as organizações desejarão atingir completamente o grau de risco *Habilitado*, pois talvez tenham que pesar os custos em relação à visão que têm dos benefícios potenciais. Cabe à alta direção e à equipe de gerentes determinar até que ponto desse processo contínuo desejarão chegar.

Além da Maturidade de Riscos da organização, a extensão da avaliação de riscos que a própria auditoria interna deve realizar também depende do grau e da velocidade das mudanças estratégicas e organizacionais.

Conclusão

A ABR não impede o uso de auditorias baseadas em sistemas e/ou processos, conforme as circunstâncias exijam. É, porém, uma abordagem que focaliza as questões que realmente interessam à organização e fornece garantias em relação ao arcabouço *(framework)* de gestão de riscos adotado pela empresa. A Auditoria Baseada em Riscos possibilita que a auditoria interna se ligue diretamente a esse *framework* de gestão de riscos, alavancando dessa forma as sinergias.

Leitura complementar

Aos interessados em utilizar a ABR como uma nova maneira de ampliar as sinergias entre todas as auditorias internas (financeiras, da qualidade, ambiental, da segurança da informação, da segurança e saúde no trabalho, etc.) conduzidas em suas organizações, recomendo a leitura do artigo: Auditoria Baseada em Riscos: mudando o paradigma das auditorias internas.

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.