# DECLARAÇÃO DE POSICIONAMENTO DO IIA: O PAPEL DA AUDITORIA INTERNA NO GERENCIAMENTO DE RISCOS CORPORATIVO

## Introdução

A importância de uma sólida governança corporativa no gerenciamento de risco tem sido progressivamente reconhecida. As organizações estão sofrendo pressão para identificar todos os riscos do negócio que elas enfrentam: social, ético e ambiental, assim como financeiro e operacional, e para explicar como elas gerenciam tais riscos a um nível aceitável. Ao mesmo tempo, a utilização de estruturas de gerenciamento de riscos corporativo tem se expandido, à medida que as organizações reconhecem suas vantagens em comparação a abordagens menos coordenadas de gerenciamento de riscos. A auditoria interna, tanto nas funções de avaliação (*asssurance*) quanto de consultoria, contribui para o gerenciamento de riscos de uma variedade de formas.

## O que é Gerenciamento de Riscos Corporativo?

As pessoas empreendem atividades de gerenciamento de riscos para identificar, avaliar, administrar e controlar todos os tipos de eventos ou situações. Estes podem variar desde simples projeções até tipos de riscos muito bem definidos, p.ex.: de risco de mercado, até ameaças e oportunidades enfrentadas pela organização como um todo. Os princípios apresentados nesta declaração podem ser utilizados para orientar o envolvimento da auditoria interna em todas as formas de gerenciamento de riscos, mas estamos particularmente interessados no gerenciamento de riscos corporativo, pois este irá, provavelmente, aperfeiçoar os processos de governança de uma organização.

**Gerenciamento de riscos corporativo - GRC (Enterprise-wide risk management - ERM)** é um processo estruturado, consistente e contínuo que percorre toda a organização para identificar, avaliar, decidir quais as respostas e reportar as oportunidades e ameaças que afetam o cumprimento de seus objetivos.

## Responsabilidade pelo GRC

O conselho tem a responsabilidade global em assegurar que os riscos são gerenciados. Na prática, o conselho delegará a operação da estrutura de gerenciamento de risco para o time de administradores que será responsável pelo cumprimento das atividades abaixo. Pode haver uma função separada que coordene e faça o gerenciamento de projeto destas atividades e forneça habilidades e conhecimentos especializados.

Todos na organização desempenham um papel para garantir o sucesso do gerenciamento de riscos corporativo, mas a responsabilidade principal na identificação dos riscos e seu gerenciamento está depositada na administração.

## Benefícios do GRC

O GRC pode fazer uma grande contribuição no sentido de auxiliar uma organização a gerenciar os riscos relacionados ao cumprimento de seus objetivos. Estes benefícios incluem:

- Maior probabilidade de alcançar tais objetivos;
- Reporte consolidado de diferentes riscos no nível do conselho;

- Compreensão melhorada dos principais riscos e suas maiores implicações;
- Identificação e compartilhamento dos riscos que percorrem o negócio;
- Maior foco da administração em questões que realmente são importantes;
- Menos surpresas ou crises;
- Maior foco interno para se fazer as coisas certas da forma certa;
- Aumento da probabilidade de iniciativas de mudanças terem sucesso;
- Capacidade de assumir maiores riscos para maiores recompensas e
- Processos de aceitação de riscos e de tomada de decisão melhor informados.

**As atividades incluídas no GRC**

- Articular e comunicar os objetivos da organização;
- Determinar o apetite de risco da organização;
- Estabelecer um ambiente interno apropriado, incluindo-se a estrutura de gerenciamento de risco;
- Identificar as potenciais ameaças ao cumprimento dos objetivos;
- Avaliar o risco (i.e., o impacto e a probabilidade da ameaça ocorrer);
- Selecionar e implantar respostas aos riscos;
- Empreender controle e outras atividades como resposta aos riscos;
- Comunicar as informações sobre os riscos de forma consistente em todos os níveis da organização;
- Monitorar e coordenar centralizadamente os processos e resultados do gerenciamento de risco e
- Fornecer avaliação (*assurance*) quanto à eficácia com que os riscos são gerenciados.

**Fornecer Avaliação (*Assurance*) do GRC**

Um dos principais requerimentos do conselho, ou seu equivalente, é obter a avaliação (*assurance*) de que os processos de gerenciamento de risco estão funcionando eficazmente e que os principais riscos estão sendo gerenciados a um nível aceitável.

É provável que a avaliação (*assurance*) venha de fontes diferentes. Entre elas, a avaliação (*assurance*) pela administração é fundamental. Isto deveria ser complementado pelo fornecimento de avaliação objetiva (*objective assurance*), a qual a atividade de auditoria interna é uma das fontes principais. Outras fontes incluem auditores externos e revisões de especialistas independentes. Os auditores internos irão normalmente fornecer avaliações (*assurances*) em três áreas:

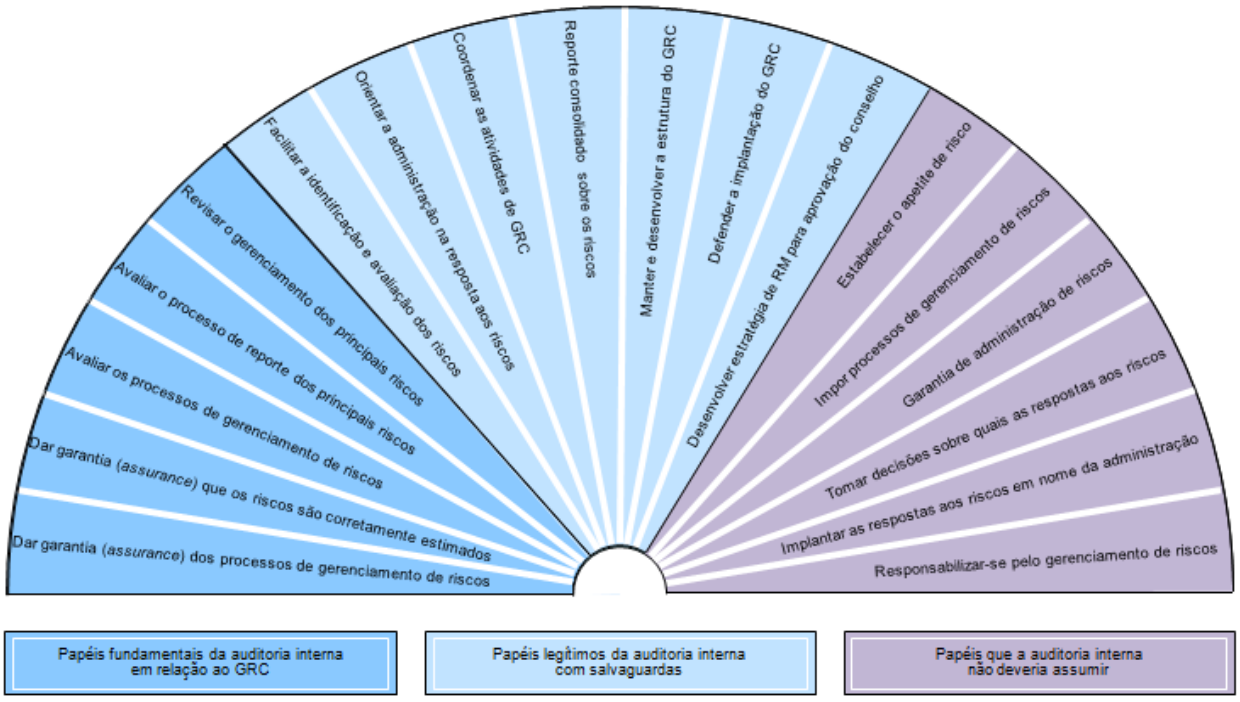
- Processos de gerenciamento de risco, tanto no seu desenho, quanto em quão bem eles estão operando;
- Gerenciamento daqueles riscos classificados como “principais” (*key*), incluindo a eficácia dos controles e outras respostas aos riscos; e
- Avaliação adequada e confiável dos riscos e reporte da situação do risco e do controle.

## O papel da auditoria interna no GRC

A auditoria interna é uma atividade independente, de avaliação (*assurance*) e de consultoria. Seu papel fundamental em relação ao GRC é fornecer avaliação objetiva (*objective assurance*) ao conselho quanto à eficácia do gerenciamento de riscos. De fato, pesquisas têm mostrado que o conselho de diretores e auditores internos concordam que as duas formas mais importantes da auditoria interna prover valor à organização são fornecer avaliação objetiva (*objective assurance*) de que os maiores riscos do negócio são gerenciados adequadamente e fornecer a avaliação (*assurance*) de que a estrutura de gerenciamento de riscos e controle interno está operando eficazmente[1].

A *Figura 1* apresenta a abrangência das atividades de GRC e indica quais papéis uma atividade profissional eficaz de auditoria interna deveria, e igualmente importante, não deveria assumir. Os principais fatores a serem considerados ao se determinar o papel da auditoria interna são: se a atividade oferece quaisquer riscos à independência e objetividade da atividade da auditoria interna; e se possivelmente aperfeiçoa os processos de gerenciamento de riscos, controle e governança da organização.

**Figura 1 – O papel da auditoria interna no GRC**




As atividades à esquerda na *Figura 1* são todas atividades de avaliação (*assurance*). Elas fazem parte do objetivo mais amplo de fornecer uma avaliação (*assurance*) do gerenciamento de risco. Uma atividade de auditoria interna em conformidade com as

[1] A Agenda de Valor (The Value Agenda), Institute of Internal Auditors – UK e Irlanda e Deloitte & Touche 2003

*Normas Internacionais para a Prática Profissional de Auditoria Interna* pode, e deveria, desempenhar pelo menos algumas destas atividades.

A auditoria interna pode prestar serviços de consultoria que melhorem os processos de governança, gerenciamento de riscos e controle de uma organização. A extensão da consultoria por um auditor interno no GRC irá depender dos outros recursos, internos e externos, disponíveis ao conselho e da maturidade de risco[2] da organização e é provável variar com o passar do tempo. A perícia do auditor interno em considerar os riscos, em compreender as conexões entre riscos e governança e em facilitação, significa que a atividade de auditoria interna está bem qualificada para atuar como um defensor e até mesmo como o gerente de projeto de GRC, especialmente nos primeiros estágios de sua implantação. À medida que a maturidade de risco da organização evolua e o gerenciamento de riscos torna-se mais inserido nas operações do negócio, o papel da auditoria interna em defender o GRC pode ser reduzido. Similarmente, se uma organização emprega os serviços de um especialista ou função de gerenciamento de riscos, a auditoria interna mais provavelmente proporcionará valor ao se concentrar em seu papel de avaliação (*assurance*), do que assumindo mais atividades de consultoria. Entretanto, se a auditoria interna ainda não tiver adotado uma abordagem baseada em risco, representada pelas atividades de avaliação (*assurance*) descritas à esquerda da *Figura 1*, é improvável que esteja apta a desempenhar as atividades de consultoria descritas no centro da figura.

**Papéis de Consultoria**

O centro da *Figura 1* mostra os papéis de consultoria que a auditoria interna pode assumir em relação ao GRC. De forma geral quanto mais à direita no mostrador a auditoria interna aventurar-se, maiores são as salvaguardas requeridas para assegurar que sua independência e objetividade sejam mantidas. Alguns dos papéis de consultoria que a atividade de auditoria interna pode assumir são:

- Disponibilizar para a administração as ferramentas e técnicas utilizadas pela auditoria interna para analisar riscos e controles;
- Ser o defensor da implantação do GRC na organização, alavancar sua especialização no gerenciamento de riscos e controles e seu conhecimento global da organização:
- Prover aconselhamento, facilitar grupos de discussão (*workshops*), orientar a organização sobre risco e controle e promover o desenvolvimento de uma linguagem, estrutura e entendimento comuns;
- Atuar como um ponto central de coordenação, monitoramento e reporte de riscos; e
- Dar suporte ao trabalho da administração na identificação da melhor forma de se mitigar um risco.

O fator principal na decisão quanto a se os serviços de consultoria são compatíveis com o papel de avaliação (*assurance*) é determinar se o auditor interno está assumindo qualquer responsabilidade que seja da administração. No caso do GRC, a auditoria

[2] Declaração de Posicionamento da Auditoria Interna Baseada em Risco de 2003 do IIA-UK e Irlanda

interna pode prestar serviços de consultoria, contanto que não tenha nenhum papel de gerenciar os riscos de fato – já que isto é responsabilidade da administração – e contanto que a alta administração ativamente endosse e dê suporte ao GRC. Recomendamos que, quando uma atividade de auditoria interna atuar no auxílio à equipe da administração na configuração ou aperfeiçoamento dos processos de gerenciamento de riscos, seu planejamento de trabalho deveria incluir uma estratégia clara e um cronograma para migrar a responsabilidade destes serviços para membros da equipe da administração.

**Salvaguardas**

A auditoria interna pode estender seu envolvimento no GRC, como mostra a *Figura 1*, desde que aplicadas algumas condições. As condições são:

- Deveria estar claro que a administração permanece como a responsável pelo gerenciamento de riscos.
- A natureza das responsabilidades do auditor interno deveria estar documentada no estatuto de auditoria interna e aprovada pelo comitê de auditoria.
- A auditoria interna não deveria gerenciar nenhum dos riscos em nome da administração.
- A auditoria interna deveria prover aconselhamento, provocar e dar suporte ao processo de tomada de decisão da administração, como oposição a tomar ela própria decisões sobre o gerenciamento de riscos.
- A auditoria interna também não pode dar avaliação objetiva (*objective assurance*) em qualquer parte da estrutura de GRC pela qual ela seja responsável. Tal avaliação (*assurance*) deve ser fornecida por outras partes convenientemente qualificadas.
- Qualquer trabalho além das atividades de avaliação (*assurance*) deveria ser reconhecido como trabalho de consultoria e as normas de implantação relativas a tais tipos de trabalhos deveriam ser seguidas.

**Habilidades e corpo de conhecimento**

Os auditores internos e gerentes de risco compartilham alguns conhecimentos, habilidades e valores. Ambos, por exemplo, compreendem os requerimentos de governança corporativa; possuem habilidades em gerenciamento de projetos, análise e facilitação e prezam o equilíbrio saudável de risco, ao invés de se assumir riscos extremos ou de assumir um comportamento de se evitar riscos. Entretanto, os gerentes de risco, como tal, servem tão somente à administração da organização e não têm que prover avaliação objetiva (*objective assurance*) e independente ao comitê de auditoria. Tão pouco os auditores internos que buscam estender seu papel no GRC deveriam subestimar as áreas de conhecimento especializadas dos gerentes de riscos (tais como: transferência de risco e técnicas de quantificação e modelagem de riscos), as quais estão fora do corpo de conhecimento da maioria dos auditores internos. Qualquer auditor interno que não possa demonstrar as habilidades e conhecimentos apropriados não deveria assumir um trabalho na área de gerenciamento de riscos. Além disso, o líder de auditoria interna não deveria prover serviços de consultoria nesta área se as

habilidades e conhecimentos adequados não estão disponíveis dentro da atividade de auditoria interna e não possam ser obtidos de outra forma.

**Conclusão**

O gerenciamento de riscos é um elemento fundamental de governança corporativa. A administração é a responsável pelo estabelecimento e operação da estrutura de gerenciamento de riscos, por nomeação do conselho. O gerenciamento de riscos corporativo produz muitos benefícios, como resultado de sua abordagem estruturada, consistente e coordenada. O papel fundamental do auditor interno em relação ao GRC deveria ser o de prover avaliação (*assurance*) à administração e ao conselho quanto à eficácia do gerenciamento de riscos. Quando a auditoria interna estende suas atividades além deste papel fundamental, deveria aplicar determinadas salvaguardas, incluindo considerar os trabalhos como serviços de consultoria e, portanto, aplicar todas as Normas relevantes. Desta forma, a auditoria interna irá proteger a sua independência e objetividade dos seus serviços de avaliação (*assurance*). Dentro destas restrições, o GRC pode auxiliar a ampliar o perfil e aumentar a eficácia da auditoria interna.

**Definição de Termos**

***Apetite de Risco:*** O nível de risco que uma organização está disposta a aceitar.

***Conselho:*** Um conselho é um corpo diretivo da organização, tais como: conselho de diretores, conselho de supervisão, responsável por uma agência ou corpo legislativo, conselho de gestores ou curadores de uma organização sem fins lucrativos ou qualquer outro corpo nomeado na organização, incluindo o comitê de auditoria, a quem o executivo chefe de auditoria pode funcionalmente se reportar.

***Controle:*** Qualquer ação tomada pela administração, conselho ou outras partes para gerenciar os riscos e aumentar a probabilidade de que os objetivos e metas estabelecidos serão alcançados. A administração planeja, organiza e dirige a execução de ações suficientes para prover razoável certeza de que os objetivos e metas serão alcançados.

***Corporação/corporativo:*** Qualquer organização estabelecida para cumprir um conjunto de objetivos.

***Defensor (Champion):*** Alguém que dá suporte e defende uma pessoa ou causa. Portanto, um defensor do gerenciamento de riscos irá promover seus benefícios, instruir a administração e quadro de funcionários de uma organização nas ações que eles precisam tomar para implantá-lo e irá encorajá-los e apoiá-los a executar essas ações.

***Estrutura de Gerenciamento de Riscos:*** A totalidade das estruturas, metodologia, procedimentos e definições que uma organização tenha escolhido utilizar para implantar os seus processos de gerenciamento de riscos.

***Facilitação:*** Trabalhar com um grupo (ou indivíduo) para tornar mais fácil ao grupo (ou indivíduo) cumprir os objetivos que o grupo tenha concordado para a reunião ou atividade. Isto envolve ouvir, instigar, observar, questionar e apoiar o grupo e seus membros. Isto não envolve fazer o trabalho ou tomar decisões.

***Gerenciamento de riscos corporativo - GRC (Enterprise-wide Risk Management - ERM):*** Um processo estruturado, consistente e contínuo que percorre toda a organização para identificar, avaliar, decidir quais as respostas e reportar as oportunidades e ameaças que afetam o cumprimento de seus objetivos.

***Maturidade de Risco:*** A extensão com a qual uma abordagem robusta de gerenciamento de risco tenha sido adotada e aplicada, como planejado, pela administração através de toda a organização para identificar, avaliar, decidir quais as respostas e reportar as oportunidades e ameaças que afetam o cumprimento dos objetivos da organização.

***Processos de Gerenciamento de Riscos:*** Processos para identificar, avaliar, administrar e controlar potenciais eventos ou situações, para fornecer uma razoável certeza em relação ao cumprimento dos objetivos da organização.

***Respostas aos Riscos:*** Os meios pelos quais uma organização escolhe gerenciar riscos individuais. As principais categorias são: tolerar o risco; tratá-lo ao mitigar seu impacto ou sua probabilidade; transferi-lo para outra organização ou encerrar a atividade que o está criando. Controles internos são uma das maneiras de se tratar um risco.

***Risco:*** A possibilidade de ocorrer um evento que venha a ter impacto no cumprimento dos objetivos. O risco é medido em termos de impacto e de probabilidade.

***Serviços de Avaliação* (*Assurance*):** Exame objetivo da evidência com o propósito de fornecer para a organização uma avaliação independente sobre os processos de governança, gerenciamento de riscos e controle. Exemplos podem incluir trabalhos de auditoria financeira, de desempenho, de conformidade, de segurança de sistemas e de "*due diligence*".

***Serviços de Consultoria:*** Atividades de aconselhamento e serviços relacionados prestados ao cliente, cuja natureza e escopo são acordados com o cliente e se destinam a adicionar valor e aperfeiçoar os processos de governança, gerenciamento de riscos e controle da organização, sem que o auditor interno assuma qualquer responsabilidade que seja da administração. Exemplos incluem orientação, assessoria, facilitação e treinamento.

***