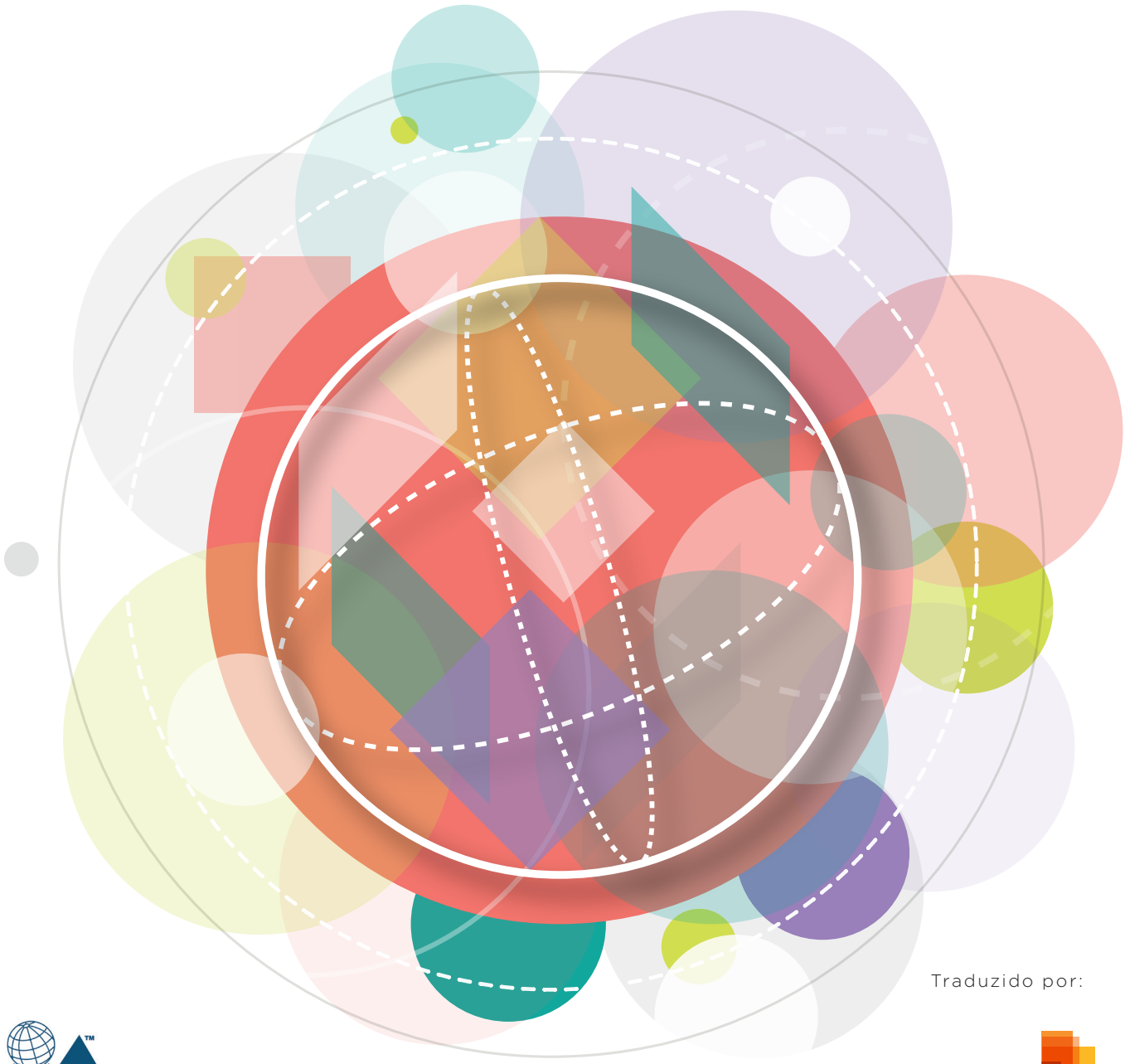
COSO

Committee of Sponsoring Organizations of the Treadway Commission

# Gerenciamento de Riscos Corporativos
## Integrado com Estratégia e Performance

(Tradução livre do original em inglês)

**Sumário Executivo**



Traduzido por:

IA Brasil

**Junho de 2017**

pwc

Este projeto foi efetuado pelo *Committee of Sponsoring Organizations of the Treadway Commission* (COSO), cujo propósito é fornecer liderança no desenvolvimento de *frameworks* abrangentes e orientação sobre controles internos, gerenciamento de riscos corporativos e prevenção a fraudes, desenhados para aprimorar a performance e a supervisão organizacional e reduzir a extensão das fraudes nas organizações. COSO é uma iniciativa do setor privado, patrocinado e financiado por:

- *American Accounting Association* (AAA)
- *American Institute of Certified Public Accountants* (AICPA)
- *Financial Executives International* (FEI)
- *Institute of Management Accountants* (IMA)
- *The Institute of Internal Auditors* (IIA)

# Introdução à edição brasileira

Temos a satisfação de apresentar a edição em português do Sumário Executivo do COSO – Gerenciamento de Riscos Corporativos – Integrado com Estratégia e Performance, emitido pelo *Committee of Sponsoring Organization of the Treadway Commission* (COSO), com a colaboração da PwC.

Esta publicação pretende constituir um modelo conceitual para gerenciamento de riscos corporativos, útil para as organizações no desenvolvimento e na manutenção de práticas alinhadas com suas estratégias e objetivos e adaptadas a ambientes de negócios cada vez mais complexos, globais e altamente dependentes de tecnologia.

Destinada aos profissionais de auditoria interna, auditoria externa, controles internos, gestão de riscos, órgãos reguladores, conselheiros e administradores em geral, esse material foi elaborado pela PwC em conjunto com o Instituto dos Auditores Internos do Brasil (IIA Brasil).

Agradecemos a todos os que participaram deste projeto, ajudando a difundir os conceitos de gerenciamento de riscos corporativos definidos pelo COSO.

Evandro Carreras
Sócio líder de Risk Assurance
PwC Brasil

Braselino Carlos da A. Sousa da Silva, CRMA
Diretor Geral
IIA Brasil

Jerri Ribeiro
Sócio de Riscos e Compliance
e coordenador do projeto
PwC Brasil

# Prefácio

Em 2004, o COSO (*Committee of Sponsoring Organizations of the Treadway Commission*) publicou a obra Gerenciamento de Riscos Corporativos – Estrutura Integrada (*Enterprise Risk Management – Integrated Framework)*, também denominado nesta tradução como COSO ERM 2004. Na última década, esse documento obteve ampla aceitação por organizações que buscavam gerenciar melhor seus riscos. No entanto, nesse mesmo período, a complexidade dos riscos mudou, novos riscos surgiram e conselheiros e executivos de empresas aprimoraram seu conhecimento e supervisão sobre as atividades de gerenciamento de riscos, passando a demandar o aperfeiçoamento dos processos de divulgação dos riscos. Esta atualização da publicação de 2004 trata da evolução do gerenciamento de riscos corporativos e da necessidade das organizações de aperfeiçoar suas abordagens de gerenciamento de riscos em um ambiente de negócios em contínua evolução.

Esta versão atualizada, agora intitulada Gerenciamento dos Riscos Corporativos – Integrado com Estratégia e Performance (*Enterprise Risk Management – Integrating with Strategy and Performance*), também denominado nesta tradução como *Framework*, ressalta a importância de se considerar o risco tanto no processo de definição das estratégias como na melhoria da performance. A primeira parte da publicação atualizada apresenta uma perspectiva sobre conceitos atuais e em desenvolvimento e aplicações do gerenciamento de riscos corporativos. Na segunda parte, o *Framework* está organizado em cinco componentes de fácil compreensão que harmonizam diferentes pontos de vista e estruturas operacionais, e melhoram as estratégias e a tomada de decisões. Em resumo, esta atualização:

- elucida o valor do gerenciamento de riscos corporativos ao estabelecer e executar uma estratégia;
- intensifica o alinhamento entre performance e gerenciamento de riscos corporativos, com o objetivo de aperfeiçoar a definição de metas de performance e o entendimento do impacto do risco sobre a performance;
- contempla as expectativas relativas a governança e supervisão;
- reconhece a globalização dos mercados e das operações e a necessidade de aplicar uma abordagem comum, embora adaptada, a todas as regiões geográficas;
- apresenta novas formas de interpretar riscos ao definir e atingir objetivos no contexto de maior complexidade dos negócios;
- amplia os aspectos de divulgação dos riscos para atender às expectativas dos *stakeholders* em relação a maior transparência;
- contempla tecnologias evolutivas e a proliferação de dados e análises de dados (*analytics*) que suportam no apoio à tomada de decisões;
- estabelece definições básicas, componentes e princípios para todos os níveis da organização envolvidos no desenho, na implementação e na execução das práticas de gerenciamento de riscos corporativos.

Os leitores também poderão consultar uma publicação complementar a esta, Controle Interno – Estrutura Integrada (*Internal Control – Integrated Framework*). As duas publicações são distintas, têm focos diferentes e não substituem uma a outra, sendo complementares. O documento Controle Interno - Estrutura Integrada abrange controles internos, que são mencionados em parte nesta publicação. O documento anterior, portanto, se mantém atual e apropriado para o desenho, implementação, execução e avaliação dos controles internos, assim como para os temas de divulgação correlatos.

O conselho do COSO aproveita a oportunidade para agradecer à PwC por suas significativas contribuições no desenvolvimento da publicação Gerenciamento de Riscos Corporativos – Integrado com Estratégia e Performance e documentos relacionados. A atenção integral da PwC aos comentários e sugestões fornecidos pelos muitos *stakeholders* e seus *insights* foram fundamentais para assegurar que os pontos fortes da publicação original fossem preservados, atualizados e aprimorados sempre que necessário. Juntos, o conselho do COSO e a PwC também agradecem ao conselho consultivo e aos observadores por suas contribuições na revisão do documento e pelos *feedbacks* fornecidos.

Robert B. Hirth Jr.
*COSO Chair*

Dennis L. Chesley
*PwC Project Lead Partner and Global and APA Risk and Regulatory Leader*

# *Committee of Sponsoring Organizations of the Treadway Commission*

## Membros do conselho

**Robert B. Hirth Jr.**
*COSO Chair*

**Richard F. Chambers**
*The Institute of Internal Auditors*

**Mitchell A. Danaher**
*Financial Executives International*

**Charles E. Landes**
*American Institute of Certified Public Accountants*

**Douglas F. Prawitt**
*American Accounting Association*

**Sandra Richtermeyer**
*Institute of Management Accountants*

# *PwC – Author*

## Principais colaboradores

**Miles E.A. Everson**
*Engagement Leader and Global and Asia, Pacific, and Americas (APA) Advisory Leader*
*New York, USA*

**Dennis L. Chesley**
*Project Lead Partner and Global and APA Risk and Regulatory Leader*
*Washington DC, USA*

**Frank J. Martens**
*Project Lead Director and Global Risk Framework and Methodology Leader*
*British Columbia, Canada*

**Matthew Bagin**
*Director*
*Washington DC, USA*

**Hélène Katz**
*Director*
*New York, USA*

**Katie T. Sylvis**
*Director*
*Washington DC, USA*

**Sallie Jo Perraglia**
*Manager*
*New York, USA*

**Kathleen Crader Zelnik**
*Manager*
*Washington DC, USA*

**Maria Grimshaw**
*Senior Associate*
*New York, USA*

# *A mudança no cenário de risco*

A compreensão da natureza do risco, a arte e a ciência da escolha, está no cerne da economia moderna. Cada escolha que fazemos quando buscamos atingir um objetivo tem seus riscos. Das decisões operacionais do dia a dia aos *trade-offs* fundamentais na reunião do conselho, lidar com o risco nessas escolhas faz parte do processo decisório.

Quando avaliamos as escolhas possíveis, raramente as decisões são binárias, implicando uma resposta certa ou errada. É por esse motivo que podemos chamar o gerenciamento de riscos corporativos de arte e de ciência. Quando avaliamos os riscos durante o processo de definição da estratégia e dos objetivos de negócios de uma organização, o gerenciamento de riscos corporativos ajuda na otimização dos resultados.

Nossa compreensão de risco e nossa prática de gerenciamento de riscos corporativos melhoraram muito nas últimas décadas. No entanto, a margem para erro é cada vez menor. O Fórum Econômico Mundial mencionou a "crescente volatilidade, complexidade e ambiguidade do mundo atual." [1] É um fenômeno que todos reconhecemos. As organizações se deparam com desafios que afetam a confiabilidade, a relevância e a confiança. Os *stakeholders* são mais atuantes hoje, demandam maior transparência e responsabilidade no gerenciamento do impacto do risco e avaliam criticamente a capacidade da liderança de identificar e concretizar oportunidades. Até mesmo o sucesso pode acarretar um risco adicional: o de não conseguir atender uma demanda inesperadamente alta ou de não manter o dinamismo esperado da empresa, por exemplo.

As organizações precisam ser mais adaptáveis à mudança. Elas precisam pensar estrategicamente em como gerir a crescente volatilidade, complexidade e ambiguidade do mundo, sobretudo nos níveis superiores da administração e no conselho, que fazem apostas mais elevadas.

Gerenciamento de Riscos Corporativos – Integrado com Estratégia e Performance fornece uma estrutura para conselhos e executivos de organizações de todos os tamanhos, partindo do nível de gerenciamento de riscos existente no curso normal dos negócios. Além disso, demonstra de que maneira a integração das práticas de gerenciamento de riscos corporativos ajuda a acelerar o crescimento e melhorar a performance. Também estabelece princípios que podem ser aplicados desde a tomada de decisões estratégicas até a performance.

A seguir descrevemos porque faz sentido para executivos e conselhos adotar a estrutura de gerenciamento de riscos corporativos,[2] o que organizações já conseguiram com sua aplicação e que outros benefícios podem ser obtidos por meio de sua aplicação contínua. Ao final do presente documento, apresentamos um olhar sobre o futuro.

## Guia da administração para o gerenciamento de riscos corporativos

Cabe à administração a responsabilidade por gerenciar os riscos da organização, porém é importante que a administração vá além: é preciso intensificar o diálogo com o conselho e os *stakeholders* sobre o uso do gerenciamento de riscos corporativos para obter vantagem competitiva. O ponto de partida é a aplicação das competências de gerenciamento de riscos corporativos no processo de escolha e refinamento da estratégia.

Cabe ressaltar que, nesse processo, a administração terá a oportunidade de melhorar seu entendimento sobre como a discussão explícita do risco afeta a definição da estratégia. O gerenciamento de riscos corporativos enriquece o diálogo da administração ao enfatizar os pontos fortes e fracos de uma estratégia, à medida que as condições se alteram, e o grau de adequação da estratégia à missão e visão da organização. Ele proporciona à administração mais segurança em relação ao fato de que estratégias alternativas foram consideradas e de que seus impactos foram avaliados por membros da organização que executarão a estratégia selecionada.

---

1 *The Global Risks Report 2016*, 11ª edição, Fórum Econômico Mundial (2016).

2 O *Framework* usa o termo "conselho de administração" ou "conselho" abrangendo o órgão de direção, órgão de supervisão, conselho diretor, sócios ou proprietários.

Uma vez definida a estratégia, o gerenciamento de riscos corporativos constitui um meio eficaz para a administração cumprir seu papel, uma vez que a organização demonstra estar atenta aos riscos que podem afetar sua estratégia e apta a gerenciá-los. A utilização do gerenciamento de riscos corporativos gera confiança e proporciona segurança aos *stakeholders*, especialmente no contexto atual, que exige um nível de vigilância jamais visto sobre como o risco é tratado e gerenciado.

## Guia do conselho para gerenciamento de riscos corporativos

Todo conselho tem um papel de supervisão, ajudando a suportar a criação de valor em uma entidade e a impedir seu declínio. Historicamente, o gerenciamento de riscos corporativos exerceu um papel expressivo no apoio ao conselho. Agora, o que se espera cada vez mais é que os conselhos supervisionem as atividades de gerenciamento de riscos corporativos.

O *Framework* traz considerações importantes para que os conselhos possam definir e tratar suas responsabilidades de supervisão dos riscos. Essas considerações incluem governança e cultura; estratégia e definição de objetivos; performance; informação, comunicação e divulgação; e a análise e revisão das práticas para melhorar a performance da organização.

O papel do conselho na supervisão dos riscos inclui as seguintes atividades:

- revisar, questionar e colaborar com a administração em relação:
  - à estratégia proposta e ao apetite ao risco;
  - ao alinhamento da estratégia e dos objetivos de negócio com a missão, a visão e os valores fundamentais da entidade;
  - às decisões de negócio relevantes, incluindo fusões e aquisições, alocações de capital, financiamentos e dividendos;
  - à resposta a variações significativas da performance da entidade ou do portfólio de riscos;
  - às respostas aos casos de desvio em relação aos valores fundamentais;
- aprovar a remuneração e os incentivos da administração;
- participar nas relações com investidores e *stakeholders*.

No longo prazo, o gerenciamento de riscos corporativos pode também aumentar a resiliência da organização – a capacidade de se antecipar e responder a mudanças. Ele ajuda as organizações a identificar fatores que representam não apenas risco, mas também mudanças, e como essas mudanças poderiam afetar a performance e demandar revisão da estratégia. Tendo maior clareza no entendimento dos impactos da mudança, a organização pode adaptar seu plano de negócio – por exemplo, ela deve recuar defensivamente ou investir em um novo negócio? O gerenciamento de riscos corporativos proporciona o *framework* adequado para o conselho avaliar os riscos e adotar uma cultura de resiliência.

### Perguntas à administração

Todos os membros da administração – e não apenas o diretor de riscos – estão preparados para formular como o risco é considerado na definição da estratégia ou nas decisões de negócios? Qual é o apetite a risco da organização e como ele poderia influenciar uma decisão específica? As respostas a essas perguntas podem nos ajudar a entender com maior precisão o *mindset* da organização na tomada de riscos.

O conselho também pode pedir que a alta administração fale não somente dos processos de risco, mas também sobre a cultura da entidade.

Como a cultura possibilita ou inibe a tomada responsável de riscos? Como a administração monitora a cultura de riscos e quais mudanças ocorreram? À medida que as coisas mudam – e elas mudam, estando ou não no radar da entidade – como o conselho pode ter certeza de que haverá uma resposta adequada e tempestiva da administração?

## O que o gerenciamento de riscos corporativos já alcançou

COSO publicou em 2004 a obra *Enterprise Risk Management – Integrated Framework*. A finalidade era ajudar as entidades a proteger e aperfeiçoar o valor dos *stakeholders*. A filosofia da obra era a de que "o valor é maximizado quando a administração define a estratégia e os objetivos de negócio para alcançar o melhor equilíbrio possível entre crescimento e retorno, considerando os respectivos riscos, e aloca recursos de maneira eficiente e eficaz para alcançar os objetivos da organização".[3]

[3] Gerenciamento de Riscos Corporativos – Estrutura Integrada, Sumário executivo, COSO (2004).

Desde sua publicação, o COSO ERM 2004 foi usado com êxito pelo mundo todo, em todos os setores e em organizações de todos os tipos e portes, para identificar riscos, gerenciá-los de acordo com o apetite a risco definido, e contribuir para o atingimento dos objetivos. Contudo, embora muitos tenham aplicado o COSO ERM 2004 na prática, seu uso poderia ser mais extenso. O avanço poderia vir da exploração de alguns aspectos com maior profundidade e clareza, e da relação entre estratégia, risco e performance. Em resposta, a publicação do *Framework* atualizado:

- faz uma ligação mais clara entre gerenciamento de riscos corporativos e uma série de expectativas dos stakeholders;
- posiciona o risco no contexto da performance da organização, e não como foco de um raciocínio isolado;
- permite às organizações se antecipar ao risco e tirar proveito disso, entendendo que mudanças geram oportunidades e não apenas a possibilidade de crises.

Esta atualização também atende ao pedido de maior ênfase na maneira como o gerenciamento de riscos corporativos influencia a estratégia e sua execução.

## Benefícios do efetivo gerenciamento de riscos corporativos

Todas as organizações precisam definir sua estratégia e ajustá-la periodicamente, ficando sempre atentas às oportunidades de criação de valor e aos desafios que encontram ao buscá-los. Para tanto, elas precisam do melhor *framework* possível para otimizar a estratégia e a performance.

É aí que entra o gerenciamento de riscos corporativos. Quando ele é integrado em toda a organização, podem ser obtidos muitos benefícios, entre eles:

- *Aumento do leque de oportunidades:* ao considerar todas as possibilidades – tanto os aspectos positivos como os negativos do risco – a administração pode identificar novas oportunidades e os desafios específicos relacionados às oportunidades atuais.
- *Identificação e gestão do risco na entidade como um todo:* toda entidade está sujeita a vários tipos de riscos, que podem afetar diversas partes da organização. Às vezes, um risco pode ser originário de uma parte da entidade, mas impactar outra parte. Dessa forma, a administração identifica e gerencia os riscos na entidade como um todo para manter e melhorar a performance.
- *Aumento dos resultados positivos e da vantagem com a diminuição das surpresas negativas:* o gerenciamento de riscos corporativos permite às entidades melhorar sua capacidade de identificar riscos e definir as respostas adequadas, diminuindo as surpresas e os custos ou prejuízos correspondentes e tirando proveito dos demais desdobramentos favoráveis.

### Alguns equívocos esclarecidos

Tomamos conhecimento de algumas interpretações equivocadas do COSO ERM 2004. Precisamos esclarecer alguns pontos:

Gerenciamento de riscos corporativos não é uma função nem um departamento. É a cultura, as competências e as práticas que as organizações integram à definição e à execução da estratégia, com o objetivo de gerenciar o risco na criação, na preservação e na realização de valor.

Gerenciamento de riscos corporativos é mais do que uma lista de riscos. Ele requer mais do que fazer um inventário de todos os riscos da organização. Ele é mais amplo e inclui práticas que a administração utiliza para a ativa gestão dos riscos.

Gerenciamento de riscos corporativos vai além do controle interno. Ele também trata de outros tópicos, como definição de estratégia, governança, comunicação com os *stakeholders* e mensuração da performance. Seus princípios se aplicam a todos os níveis da organização e a todas as funções.

Gerenciamento de riscos corporativos não é um *checklist*. É um conjunto de princípios com base nos quais os processos podem ser criados ou integrados para uma determinada organização. É também um sistema de monitoramento, aprendizado e melhoria da performance.

Gerenciamento de riscos corporativos pode ser usado por organizações de qualquer porte. Se a organização tiver uma missão, uma estratégia e um objetivo – e a necessidade de tomar decisões que levem em conta o risco – ela poderá aplicar o gerenciamento de riscos corporativos. Ele pode e deve ser usado por organizações de todos os tipos – de pequenas empresas a empresas locais e não lucrativas e órgãos governamentais, até empresas da lista Fortune 500.

- *Diminuição da oscilação da performance:* para algumas entidades, os desafios não são as surpresas e os prejuízos, mas sim a oscilação da performance. Uma performance além das expectativas pode causar tanta preocupação quanto uma performance aquém das expectativas. O gerenciamento de riscos corporativos permite prever os riscos que poderiam afetar a performance e colocar em prática as medidas necessárias para minimizar a disrupção e maximizar a oportunidade.
- *Melhor distribuição de recursos:* todo risco poderia ser considerado uma demanda por recursos. A obtenção de informações rigorosas sobre riscos permite que a administração, diante de recursos finitos, avalie as necessidades, priorize a distribuição e melhore a alocação de recursos.
- *Aumento da resiliência da empresa:* a viabilidade da entidade no médio e longo prazos depende de sua capacidade de prever mudanças e responder a elas – não apenas para sobreviver, mas também para evoluir e prosperar. Em parte, isso é viabilizado pela eficácia no gerenciamento de riscos corporativos e adquire importância cada vez maior à medida que se acelera o ritmo da mudança e aumenta a complexidade dos negócios.

Esses benefícios ressaltam o fato de que o risco não deve ser encarado unicamente como uma possível restrição ou obstáculo à definição e à execução de uma estratégia. Pelo contrário, a mudança trazida pela avaliação do risco e a correspondente resposta organizacional dão origem a oportunidades estratégicas e a importantes competências diferenciadoras.

## O papel do risco na definição da estratégia

Definir uma estratégia implica fazer escolhas e aceitar *trade-offs*. Sendo assim, faz total sentido aplicar o gerenciamento de riscos corporativos à estratégia, uma vez que essa é a melhor abordagem para desvendar a arte e a ciência de fazer escolhas fundamentadas.

O risco deve ser levado em conta em diversos processos de definição estratégica. No entanto, ele é avaliado costumeiramente em relação a seu possível efeito em uma estratégia anteriormente determinada. Em outras palavras, as discussões relacionam os riscos à estratégia existente: temos uma estratégia, o que poderia afetar sua relevância e viabilidade?

Mas há outras perguntas sobre estratégia que as organizações estão aprendendo a fazer melhor: modelamos corretamente a demanda dos clientes? Nossa cadeia de suprimentos entregará os pedidos nos prazos acordados e dentro do orçamento? Surgirão novos concorrentes? Nossa infraestrutura tecnológica está à altura das demandas? Esses são tipos de perguntas com as quais os executivos se defrontam todos os dias, e cujas respostas serão fundamentais para a execução da estratégia.

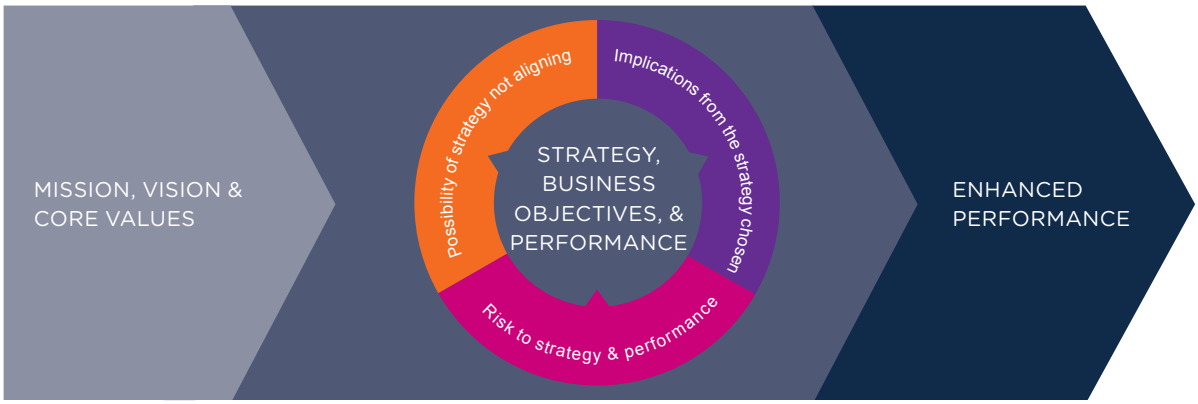
O risco da estratégia escolhida, contudo, é apenas um dos aspectos a considerar. Como este *Framework* destaca, existem dois outros aspectos do gerenciamento de riscos corporativos que podem ter um efeito muito maior sobre o valor da entidade: a possibilidade de desalinhamento e as implicações da estratégia escolhida.

O primeiro deles, **a possibilidade de desalinhamento entre a estratégia e a missão, a visão e os valores fundamentais da organização**, é essencial para as decisões que servem como base para a definição da estratégia. Toda organização tem uma missão, uma visão e valores fundamentais que definem o que ela procura atingir e como quer conduzir seus negócios. Algumas organizações demonstram ser reticentes quanto à adoção ampla dos seus códigos e valores corporativos. Entretanto, já ficou demonstrado que missão, visão e valores fundamentais são importantes – ainda mais quando se trata de gerenciar riscos e manter-se resiliente em períodos de mudanças relevantes.

A estratégia escolhida precisa suportar a missão e a visão da organização. Uma estratégia desalinhada aumenta a possibilidade de a organização não conseguir concretizar sua missão e sua visão, ou comprometer seus valores, mesmo que a estratégia seja executada satisfatoriamente. Por esses aspectos, o gerenciamento de riscos corporativos considera a possibilidade de a estratégia estar desalinhada com a missão e a visão da organização.

O outro aspecto são **as implicações da estratégia escolhida**. Quando a administração formula uma estratégia e estuda as alternativas em conjunto com o conselho, decisões são tomadas levando em conta os *trade-offs* inerentes à estratégia. Cada estratégia alternativa tem um perfil de risco próprio – essas são as implicações que emanam da estratégia. O conselho e a administração precisam determinar se a estratégia funciona levando em conta o apetite ao risco da organização e como ela direcionará a organização a definir objetivos e alocar recursos com eficiência.

Chegamos ao ponto mais importante: o gerenciamento de riscos corporativos envolve tanto entender as *implicações da estratégia e a possibilidade de seu eventual desalinhamento*, como gerenciar os riscos associados aos objetivos de negócios. A figura a seguir ilustra essas considerações no contexto da missão, visão e valores fundamentais, e como determinantes dos direcionadores estratégicos e da performance da entidade.




O gerenciamento de riscos corporativos, como vem sendo tipicamente praticado, ajudou muitas organizações a identificar, avaliar e gerenciar os riscos da estratégia. No entanto, as causas mais importantes de destruição de valor residem na possibilidade de a estratégia não suportar a missão e a visão da entidade, e nas implicações decorrentes da estratégia escolhida.

O gerenciamento de riscos corporativos destaca a escolha da estratégia. A definição de uma estratégia demanda um processo decisório estruturado que analise os riscos e alinhe os recursos com a missão e a visão da organização.

# Um *Framework* orientado

Gerenciamento de Riscos Corporativos – Integrado com Estratégia e Performance realça a importância do gerenciamento de riscos corporativos no planejamento estratégico e da sua incorporação em toda a organização – porque o risco influencia e alinha estratégia e performance em todos os departamentos e funções.


O *Framework* é um conjunto de princípios organizados em cinco componentes inter-relacionados:

1. *Governance and Culture* (Governança e cultura): a governança dá o tom da organização, reforçando a importância e instituindo responsabilidades de supervisão sobre o gerenciamento de riscos corporativos. A cultura diz respeito a valores éticos, a comportamentos esperados e ao entendimento do risco em toda a entidade.
2. *Strategy and Objective-Setting* (Estratégia e definição de objetivos): gerenciamento de riscos corporativos, estratégia e definição de objetivos atuam juntos no processo de planejamento estratégico. O apetite a risco é estabelecido e alinhado com a estratégia; os objetivos de negócios colocam a estratégia em prática e, ao mesmo tempo, servem como base para identificar, avaliar e responder aos riscos.
3. *Performance*: os riscos que podem impactar a realização da estratégia e dos objetivos de negócios precisam ser identificados e avaliados. Os riscos são priorizados com base no grau de severidade, no contexto do apetite a risco. A organização determina as respostas aos riscos e, por fim, alcança uma visão consolidada do portfólio e do montante total dos riscos assumidos. Os resultados desse processo são comunicados aos principais *stakeholders* envolvidos com a supervisão dos riscos.
4. *Review and Revision* (Análise e revisão): ao analisar sua performance, a organização tem a oportunidade de refletir sobre até que ponto os componentes do gerenciamento de riscos corporativos estão funcionando bem ao longo do tempo e no contexto de mudanças relevantes, e quais correções são necessárias.
5. *Information, Communication, and Reporting* (Informação, comunicação e divulgação): o gerenciamento de riscos corporativos demanda um processo contínuo de obtenção e compartilhamento de informações precisas, provenientes de fontes internas e externas, originadas das mais diversas camadas e processos de negócios da organização.

Os cinco componentes do novo *Framework* se combinam em um conjunto de princípios.[4] Esses princípios abrangem desde a governança até o monitoramento. Eles descrevem práticas que podem ser aplicadas de diferentes formas nas organizações, independentemente do seu tamanho, tipo ou setor econômico. A adoção dos princípios pode trazer ao conselho e à administração a segurança de que a organização é capaz de gerenciar de modo aceitável os riscos associados à estratégia e aos objetivos de negócios.

**Governance & Culture**

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

**Strategy & Objective-Setting**

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

**Performance**

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

**Review & Revision**

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in Enterprise Risk Management

**Information, Communication, & Reporting**

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

## Um olhar para o futuro

Não há dúvida de que as organizações continuarão a enfrentar um futuro repleto de volatilidade, complexidade e ambiguidade. O gerenciamento de riscos corporativos será um fator importante para a maneira como uma organização conduzirá seus negócios para prosperar em tempos de mudanças constantes. Independentemente do tipo e do tamanho da organização, é preciso que as estratégias sejam condizentes e alinhadas com sua missão. Todas as entidades precisam apresentar características que determinem respostas eficazes a mudanças, o que inclui agilidade na tomada de decisões, habilidade de responder de maneira coesa e capacidade de se adaptar e se reposicionar, mantendo durante todo esse processo altos níveis de confiança de todos os *stakeholders*.

Olhando para o futuro, podemos observar diversas tendências que terão impacto no gerenciamento de riscos corporativos. A seguir destacamos quatro delas:

- *Lidar com a proliferação de dados:* quanto mais dados forem disponibilizados e aumentar a velocidade com que eles podem ser analisados, o gerenciamento de riscos corporativos precisará se adaptar. Os dados virão de dentro e de fora da entidade e serão estruturados de diferentes formas. Ferramentas avançadas de análise e visualização de dados continuarão a evoluir e serão muito úteis para entender o risco e seu impacto, positivo e negativo.
- *Alavancar inteligência artificial e automação:* muitas pessoas reconhecem que entramos na era dos processos automatizados e da inteligência artificial. Sejam quais forem as crenças de cada um, é importante que as práticas de gerenciamento de riscos corporativos considerem o impacto dessas e de futuras tecnologias e tirem proveito de suas capacidades. Relações, tendências e padrões não reconhecíveis anteriormente podem agora ser revelados, proporcionando uma rica fonte de informações críticas para o gerenciamento do risco.
- *Administrar o custo do gerenciamento de riscos:* uma preocupação frequente de muitos executivos de negócios é o custo do gerenciamento de riscos, dos processos de conformidade e das atividades de controle, quando comparados com o valor gerado por ambos. Com a evolução das práticas de gerenciamento de riscos, será cada vez mais importante que as atividades relacionadas a risco, conformidade, controle e até governança sejam eficientemente coordenadas para proporcionar o maior benefício possível à organização. Essa pode representar uma das melhores oportunidades para o gerenciamento de riscos corporativos redefinir sua importância para a organização.

[4] Uma descrição mais completa desses vinte princípios é apresentada no fim deste documento.

- *Construir organizações mais fortes:* à medida que as organizações aprimoram sua capacidade de integrar o gerenciamento de riscos corporativos com a estratégia e a performance, surge a oportunidade de fortalecer a resiliência. Ao conhecer os riscos que terão maior impacto na entidade, as organizações podem usar o gerenciamento de riscos corporativos para apoiá-las na criação de competências que lhes permitam atuar com antecedência, criando novas oportunidades.

Em síntese, o gerenciamento de riscos corporativos precisará mudar e adaptar-se ao futuro para continuar a proporcionar os benefícios descritos no *Framework*. Com o foco adequado, os benefícios provenientes do gerenciamento de riscos corporativos superarão em muito os investimentos, dando às organizações a confiança necessária na sua capacidade de lidar com o futuro.

## Agradecimentos

Nosso agradecimento especial às seguintes empresas e organizações por permitirem a participação dos membros do conselho consultivo e observadores.

## Membros do conselho consultivo

*Empresas e organizações*

- Athene USA (Jane Karli)
- Edison International (David J. Heller)
- First Data Corporation (Lee Marks)
- Georgia-Pacific LLC (Paul Sobel)
- Invesco Ltd. (Suzanne Christensen)
- Microsoft (Jeff Pratt)
- US Department of Commerce (Karen Hardy)
- United Technologies Corporation (Margaret Boissoneau)
- Zurich Insurance Company (James Davenport)

*Ensino superior e associações*

- North Carolina State University (Mark Beasley)
- St. John's University (Paul Walker)
- The Institute of Internal Auditors (Douglas J. Anderson)

*Firmas de serviços profissionais*

- Crowe Horwath LLP (William Watts)
- Deloitte & Touche LLP (Henry Ristuccia)
- Ernst & Young (Anthony J. Carmello)
- James Lam & Associates (James Lam)
- Grant Thornton LLP (Bailey Jordan)
- KPMG LLP Americas (Deon Minnaar)
- Mercury Business Advisors Inc. (Patrick Stroh)
- Protiviti Inc. (James DeLoach)

*Ex-membro do conselho do COSO*

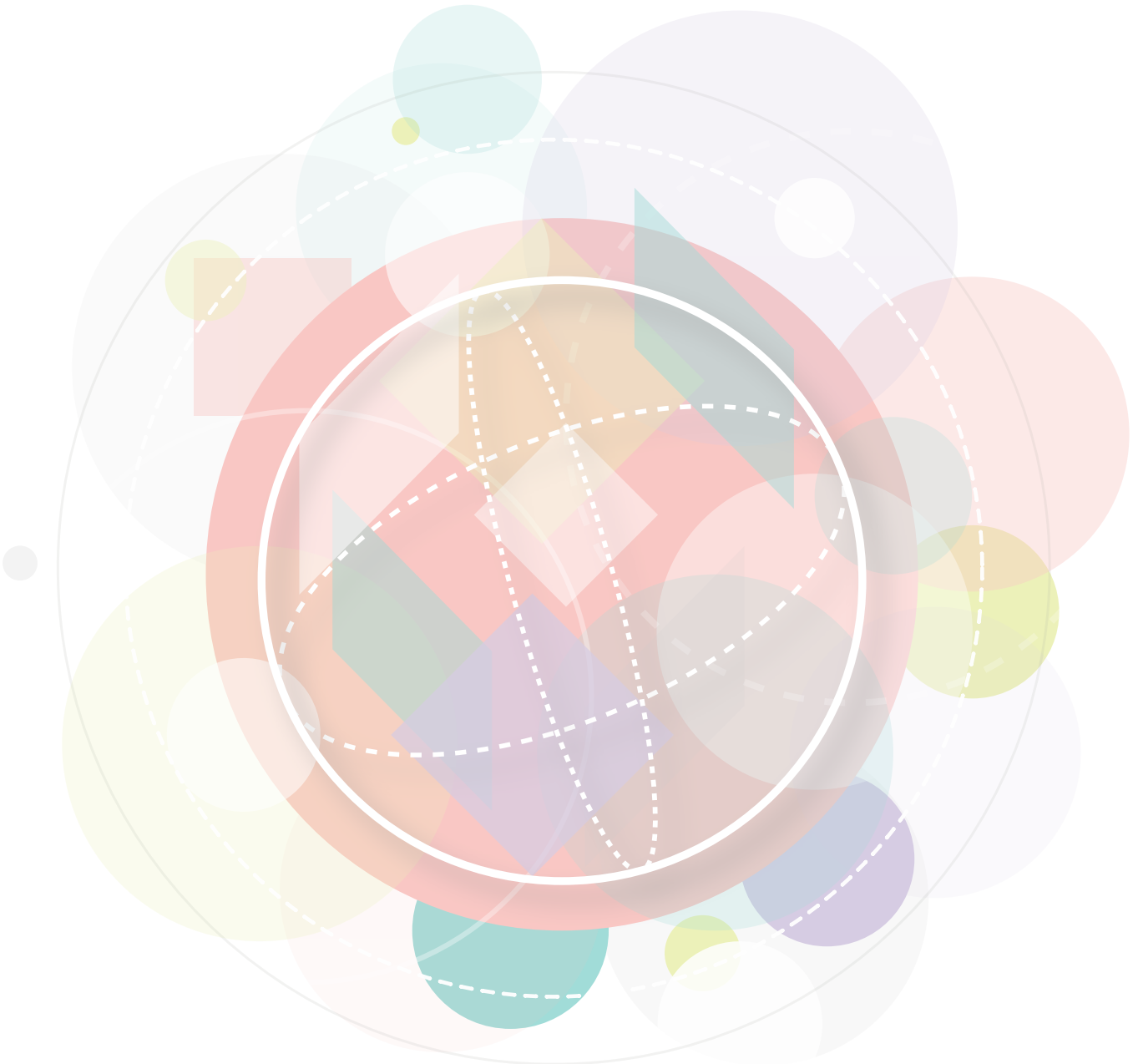
- COSO Chair, 2009–2013 (David Landsittel)

## Observadores

- Federal Deposit Insurance Corporation (Harrison Greene)
- Government Accountability Office (James Dalkin)
- Institute of Management Accountants (Jeff Thompson)
- Institut der Wirtschaftsprüfer (Horst Kreisel)
- International Federation of Accountants (Vincent Tophoff)
- ISACA (Jennifer Bayuk)
- Risk Management Society (Carol Fox)

# Componentes e princípios

1. **Exerce supervisão do risco por intermédio do conselho** — O conselho de administração supervisiona a estratégia e cumpre responsabilidades de governança para ajudar a administração a atingir a estratégia e os objetivos de negócios.
2. **Estabelece estruturas operacionais** — A organização estabelece estruturas operacionais para atingir a estratégia e os objetivos de negócios.
3. **Define a cultura desejada** — A organização define os comportamentos esperados que caracterizam a cultura desejada pela entidade.
4. **Demonstra compromisso com os valores fundamentais** — A organização demonstra compromisso com os valores fundamentais da entidade.
5. **Atrai, desenvolve e retém pessoas capazes** — A organização tem o compromisso de formar capital humano de acordo com a estratégia e os objetivos de negócios.
6. **Analisa o contexto de negócios** — A organização leva em conta os possíveis efeitos do contexto de negócios sobre o perfil de riscos.
7. **Define o apetite a risco** — A organização define o apetite a risco no contexto da criação, da preservação e da realização de valor.
8. **Avalia estratégias alternativas** — A organização avalia estratégias alternativas e seu possível impacto no perfil de riscos.
9. **Formula objetivos de negócios** —A organização considera o risco enquanto estabelece os objetivos de negócios nos diversos níveis, que se alinham e suportam a estratégia.
10. **Identifica o risco** — A organização identifica os riscos que impactam a execução da estratégia e os objetivos de negócios.
11. **Avalia a severidade do risco** — A organização avalia a severidade do risco.
12. **Prioriza os riscos** — A organização prioriza os riscos como base para a seleção das respostas a eles.
13. **Implementa respostas aos riscos** — A organização identifica e seleciona respostas aos riscos.
14. **Adota uma visão de portfólio** — A organização adota e avalia uma visão consolidada do portfólio de riscos.
15. **Avalia mudanças importantes** — A organização identifica e avalia mudanças capazes de afetar de forma relevante a estratégia e os objetivos de negócios.
16. **Analisa riscos e performance** — A organização analisa a performance da entidade e considera o risco como parte desse processo.
17. **Busca o aprimoramento no gerenciamento de riscos corporativos** — A organização busca o aprimoramento contínuo do gerenciamento de riscos corporativos.
18. **Alavanca sistemas de informação** — A organização maximiza a utilização dos sistemas de informação e tecnologias existentes na entidade para impulsionar o gerenciamento de riscos corporativos.
19. **Comunica informações sobre riscos** — A organização utiliza canais de comunicação para suportar o gerenciamento de riscos corporativos.
20. **Divulga informações de riscos, cultura e performance** — A organização elabora e divulga informações sobre riscos, cultura e performance abrangendo todos os níveis e a entidade como um todo.



A versão integral de *Enterprise Risk Management – Integrating with Strategy and Performance* está disponível para compra em www.coso.org.