Modelos de referência de gestão corporativa de riscos

A política de gestão de riscos adotada pelo TCU baseia-se nas melhores práticas internacionais sobre o tema. Conheça alguns desses modelos abaixo:

COSO-IC (COSO I)

Em 1992, o *Committee of Sponsoring Organizations of the Treadway Commission – COSO* publicou o guia *Internal Control - integrated framework (COSO-IC ou COSO I),* com o objetivo de orientar as organizações quanto a princípios e melhores práticas de controle interno, em especial para assegurar a produção de relatórios financeiros confiáveis e prevenir fraudes.

Nesse modelo, controle interno é definido como um "processo projetado e implementado pelos gestores para mitigar riscos e alcançar objetivos". Por sua vez, risco é definido como "a possibilidade de ocorrência de um evento que possa afetar o alcance dos objetivos" (COSO, 1992). Ou seja, para o COSO-IC, o controle interno é um processo que tem por objetivo mitigar riscos, com vistas ao alcance dos objetivos.

O modelo do COSO-IC é representado por um cubo no qual as três faces visíveis representam: i) tipos de objetivos; ii) níveis da estrutura organizacional e iii) componentes.

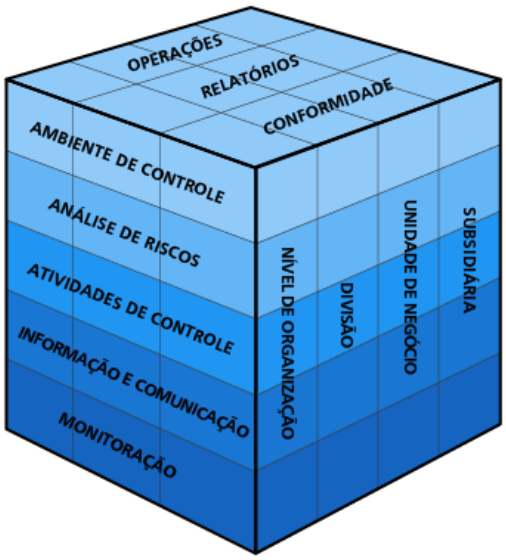


Figura Coso IC - adaptado para o português

O Coso-IC foca em três objetivos: operacionais, assegurar relatórios financeiros confiáveis e assegurar conformidade legal/regulatória. A visão relativa à estrutura organizacional busca atingir a organização como um todo, abarcando unidade, departamento, divisão, etc., ou seja, do maior ao menor nível. O modelo concentra-se nos seguintes componentes: ambiente de controle, análise de riscos, atividades de controle, informação e comunicação e monitoração.

Em resumo, as perspectivas mostradas nas três faces do cubo do COSO-IC podem ser entendidas como o conjunto de atividades, recursos e viabilizadores críticos para o processo de controle interno a ser aplicado na instituição em todos os níveis, com vistas a assegurar o alcance de certos tipos de

aplicado na instituição em todos os níveis, com vistas a assegurar o alcance de certos tipos de objetivos normalmente existentes nas organizações. Apesar da avaliação de riscos ser um componente do modelo, o foco está no processo de controle interno da organização, e não estão contempladas todas as atividades e outros aspectos importantes para a realização de um processo completo de gestão de riscos. Em outras palavras, o COSO-IC, é um modelo de controle interno que utiliza práticas de avaliação de riscos, não tendo sido elaborado com o objetivo de ser um modelo de gestão de riscos em sentido estrito.

Em 2013, uma versão atualizada do COSO-IC foi publicada, na qual destacam-se as seguintes modificações: facilitada a verificação de conformidade com a Lei Sarbanes-Oxley, generalização do objetivo relatórios financeiros para relatórios da gestão em geral e explícita articulação de 17 princípios associados aos componentes do sistema de Controle Interno.

COSO-ERM (COSO II)

Em 2004, o *COSO* publicou o *Enterprise Risk Management - integrated framework (COSO-ERM ou COSO II)*, documento que ainda hoje é tido como referência no tema gestão de riscos corporativos.

Esse modelo, como o próprio nome revela, foi projetado com o objetivo de orientar as organizações no estabelecimento de um processo de gestão de riscos corporativos e na aplicação de boas práticas sobre o tema.

Vale lembrar que o COSO-ERM é uma evolução do COSO-IC, ou seja, abrange todo o escopo do modelo anterior e incorpora ferramentas complementares, como se vê na seguinte afirmação: “[o modelo COSO-ERM] não pretende substituir o modelo do controle interno [COSO-IC], mas sim incorporá-lo" (COSO, 2004).

De acordo com o COSO-ERM, a gestão de riscos corporativos é:

> Processo que permeia toda a organização, colocado em prática pela alta administração da entidade, pelos gestores e demais colaboradores, aplicado no estabelecimento da estratégia e projetado para identificar possíveis eventos que possam afetar a instituição e para gerenciar riscos de modo a mantê-los dentro do seu apetite de risco, com vistas a fornecer segurança razoável quanto ao alcance dos objetivos da entidade (COSO, 2004, tradução livre).

Importante observação derivada da definição acima é que o processo corporativo de gestão de riscos previsto no COSO-ERM, além de ser aplicável na realização normal das atividades - operacionais, administrativas e de suporte - deveria ser aplicado também nas atividades de planejamento voltadas à definição da estratégia da organização. Isso fica ainda mais evidente quando se observa que a perspectiva do cubo do COSO-ERM relativa aos objetivos inclui um novo tipo de objetivo a ser assegurado e que não era listado no COSO-IC, qual seja, a categoria dos objetivos estratégicos.

Na perspectiva do cubo do COSO-ERM que trata dos componentes do modelo, observa-se que a atividade “análise de riscos”, anteriormente prevista no COSO-IC, foi substituída e complementada pelas seguintes atividades: identificação de eventos, avaliação de riscos e, por fim, resposta a riscos. Essas atividades devem considerar o apetite de risco e os níveis de tolerância a riscos definidos pela organização:

> Risk Response – Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the entity’s risk tolerances and risk appetite (COSO, 2004).

Característica marcante do COSO-ERM é a previsão, como parte do modelo, de um componente relacionado com a definição de objetivos, como se vê na figura do cubo que representa aquele modelo e também nas seguintes afirmações:

> An appropriate process for objective setting is a critical component of enterprise risk management… Enterprise risk management ensures that executive management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite (COSO, 2004)

O COSO-ERM introduz conceitos interessantes como apetite a risco e tolerância a riscos. O primeiro refere-se ao montante de risco que a organização dispõe-se a aceitar na criação de valor. O segundo trata do nível de variação aceitável no alcance de um certo objetivo.

Em resumo, verifica-se que o modelo COSO-ERM, ao orientar a aplicação de um processo de gestão de riscos corporativos, incorpora e aprimora o modelo COSO-IC pela inclusão de componentes e elementos adicionais que asseguram a realização de todas as atividades necessárias.

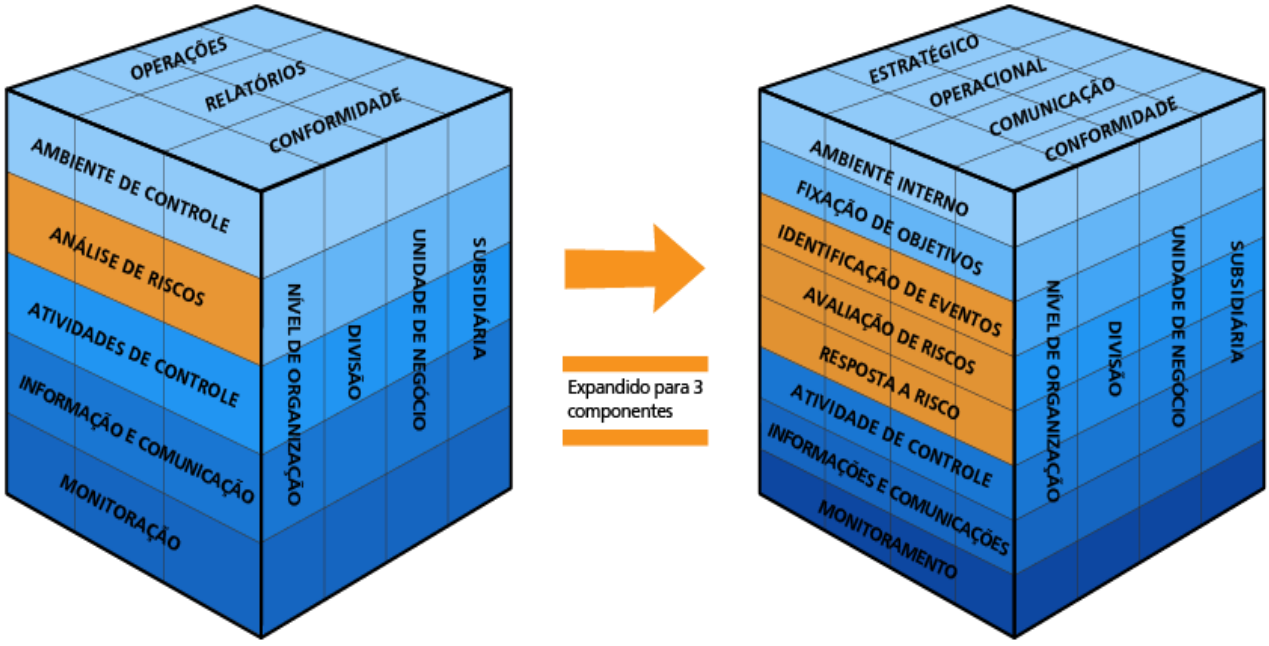


Figura (COSO - IC e Coso ERM) adaptado para o português

Vale lembrar ainda a relação existente entre controle interno, gestão de riscos corporativos e a governança corporativa, como bem definido na versão 2013 do *COSO Internal Control —Integrated Framework:*

Enterprise risk management is broader than internal control, elaborating on internal control and focusing more directly on risk. Internal control is an integral part of enterprise risk management, while enterprise risk management is part of the overall governance process (COSO, 2013).

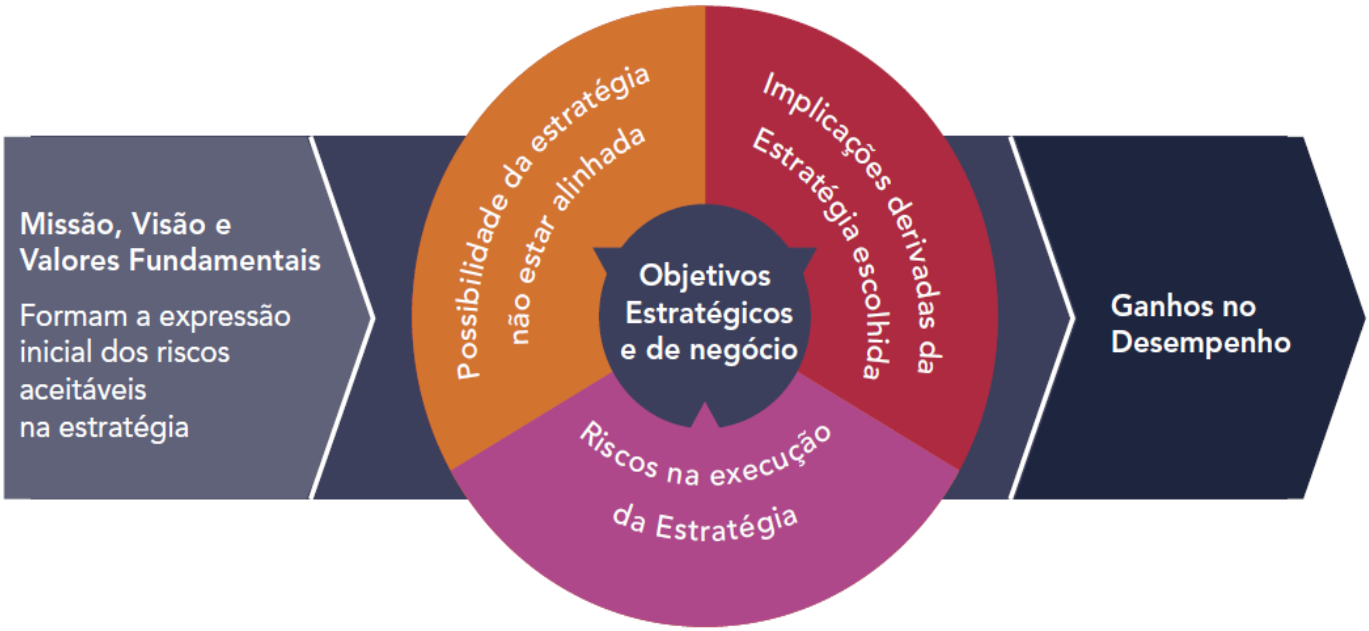
Figura adaptada para o português

COSO – ERM (COSO 2017)

A nova versão, *COSO ERM – Integrating with Strategy and Performance*, também denominado como Framework, destaca a importância de considerar os riscos tanto no processo de estabelecimento da estratégia quanto na melhoria da performance.

A primeira parte da publicação oferece uma perspectiva dos conceitos atuais e em desenvolvimento e aplicações do gerenciamento de riscos corporativos. A segunda parte da publicação apresenta 20 princípios organizados em 5 componentes inter-relacionados: Governança e cultura, Estratégia e definição de objetivos, Performance, Monitoramento do desempenho e revisão; e finalmente Informação, comunicação e divulgação.

Aderir a estes princípios pode conferir a organização uma razoável expectativa de que ela entende e se esforça para gerenciar os riscos associados à sua estratégia e objetivos de negócios.



ISO 31000:2009 e 31000:2018

A norma técnica ISO 31000:2009 resultou de esforço da *International Organization for Standardization* (ISO) para criar um padrão internacional para a gestão de riscos corporativos, tendo sido publicada no Brasil sob o nome ABNT NBR ISO 31000:2009 Gestão de riscos – Princípios e diretrizes.

O processo de gestão de riscos preconizado na ISO 31000:2009 não difere muito do que já era previsto em normas técnicas regionais que a antecederam e contempla as seguintes fases ou atividades: estabelecimento do contexto, identificação, análise, avaliação e tratamento de riscos, comunicação e consulta, monitoramento e análise crítica.

Também em 2009, a ISO publicou versão atualizada – e compatível com a ISO 31000 – do guia *ISO Guide 73 - Risk Management Vocabulary,* instrumento importante para a sedimentação de uma linguagem comum e padronizada relativa ao tema.

Em 2018, a ISO 2009 foi revisada e seu conteúdo foi totalmente substituído pela nova versão. Na essência, o processo de gestão de riscos continua o mesmo incluindo as etapas relativas às atividades de comunicação e consulta, ao estabelecimento do contexto, avaliação dos riscos (identificar, analisar e avaliar os riscos), uma etapa relativa ao monitoramento e, por fim, registro e relato dos riscos.

INTOSAI – Guias GOV 9100 e GOV 9130

A Organização Internacional de Entidades Fiscalizadoras Superiores (INTOSAI) publicou, em 2004, o guia GOV 9100 – Guidelines for Internal Control Standards for the Public Sector, com o objetivo de prover um modelo de controle interno no setor público e fornecer uma base por meio do qual o controle interno pode ser avaliado e aplicável a todos os aspectos relacionados com o funcionamento de uma organização pública.

Em 2007, a INTOSAI publicou o guia complementar GOV 9130 – *Guidelines for Internal Control Standards for the Public Sector – Further Information on Entity Risk Management*, com recomendações adicionais ao guia GOV9100. O documento preconiza um modelo para a aplicação da gestão de riscos no setor público e provê uma base no qual a gestão de riscos pode ser avaliada.

Esses guias foram baseados, respectivamente, no modelo COSO-IC e COSO-ERM anteriormente citados, com algumas modificações, especialmente adaptações de linguagem e de contexto, de forma a adequar o uso ao setor público.